FMFM 2-4

Counterintelligence

Certain provisions of this manual are the subject of an International Standardization Agreement (NATO STANAG 1059, 2022, 2033, 2044, 2084, and 2097). When amendment, revision or cancellation of this publication is proposed which will modify the international agreement concerned, the preparing activity will take appropriate action, as provided for in MCO 5711.1E, through international standardization channels to change the agreement or make other appropriate accommodations.

U.S. Marine Corps

PCN 139 000131 00

$4.00

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380

5 December 1983

FOREWORD

1. PURPOSE

FMFM 2-4, *Counterintelligence*, sets forth information and guidance concerning the planning and execution of counterintelligence activities within the Marine Corps.

2. SCOPE

This manual discusses the mission, responsibilities, organization, functions, and employment of counterintelligence assets during combat and garrison operations. Counterintelligence planning and training considerations are also discussed.

3. SUPERSESSION

This publication supersedes FMFM 2-4, *Counterintelligence* dated 15 March 1979.

4. CHANGES

Recommendations for improving this manual are invited from commands as well as directly from individuals. The attached User Suggestion Form should be utilized by individuals and forwarded to:

Commanding General
Marine Corps Development and Education Command (Code D 046)
Quantico, Virginia 22134

5. CERTIFICATION

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

D. M. TWOMEY
Major General, U.S. Marine Corps
Commanding General
Marine Corps Development and Education Command
Quantico, Virginia

DISTRIBUTION: TBD

Reviewed & approved for reprinting
by CMC (PP) on 25 Mar 1985.

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402

USER SUGGESTION FORM

From:

To: Commanding General, Marine Corps Development and Education Command (Code D 046), Quantico, Virginia 22134

Subj: FMFM 2-4, *Counterintelligence*; recommendation concerning

1. In accordance with the Foreword to FMFM 2-4, which invites individuals to submit suggestions concerning this FMFM directly to the above addressee, the following unclassified recommendation is forwarded:

Page	Article/Paragraph No.	Line No.	Figure/Table No.

Nature of Change: ☐ Add ☐ Delete ☐ Change ☐ Correct

1. Proposed New Verbatim Text: (Verbatim, double spaced; continue on additional pages as necessary.)

2. Justification/Source: (Need not be double spaced.)

NOTE:
Only one recommendation per page.

DEPARTMENT OF THE NAVY

OFFICIAL BUSINESS

PENALTY FOR PRIVATE USE $300

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 12495 WASHINGTON, D C

POSTAGE WILL BE PAID BY UNITED STATES MARINE CORPS

To: Commanding General
Marine Corps Development and Education Command
(Code D 046)
Quantico, Virginia 22134

Record of Changes

Change No.	Date of Change	Date of Entry	Organization	Signature

(reverse blank)

Counterintelligence

Table of Contents

Section 4. Counterintelligence Garrison Operations

Section 5. Counterintelligence Planning

Section 6. Counterintelligence Training

Appendixes:

Section 1

Introduction

101. General

a. Importance. Counterintelligence is that aspect of intelligence devoted to neutralizing or destroying the effectiveness of hostile foreign intelligence activities, and to the protection of information against espionage, personnel against subversion and terrorism, and installations and material against sabotage. Counterintelligence measures enhance security, aid in reducing risks to the command, and are essential in achieving surprise during military operations. Accordingly, counterintelligence provides a significant contribution to a command's operations security (OPSEC) program. As an element of intelligence, counterintelligence must be closely coordinated and thoroughly integrated with the overall intelligence effort. The success of any military operation is dependent on reliable intelligence and effective counterintelligence. Fleet Marine Force Manual (FMFM) 2-1, *Intelligence*, provides guidance for intelligence activities within the Marine Corps.

b. Basis for Counterintelligence Activities. The enemy can be expected to use every available means to thwart or otherwise impede our forces with his efforts directed towards intelligence collection, sabotage, subversion, and terrorism. Enemy intelligence collection activities are directed toward obtaining detailed knowledge of our forces and their capabilities, limitations, vulnerabilities, intentions, and probable courses of action, as well as information concerning the area of operations, including weather, terrain, and hydrography. Knowledge on the part of the enemy concerning an operation projected by friendly forces will enable him to concentrate his efforts on preparing the objective for defense, attacking friendly staging areas, and disrupting the operation through sabotage, terrorism, and subversive activities. Accordingly, counterintelligence is essential to the security of our forces from the inception of planning until the operation is completed.

Section 2

Counterintelligence Organization and Functions

201. General

Marine Corps counterintelligence teams are organized, trained, and equipped to provide combat support to the Fleet Marine Force (FMF). During peacetime, in addition to planning, preparing, and training for combat, Marine counterintelligence units also provide various counterintelligence services and support to enhance the security and readiness of the Marine Corps.

The wide range and continuing nature of counterintelligence, and its integration within the overall intelligence effort, require an understanding of the national intelligence organization as well as of the intelligence and counterintelligence units of the Armed Forces. The principal organizations concerned with intelligence and counterintelligence are summarized in the following paragraphs. (See fig. 2-1.)

202. National Intelligence Organizations

a. National Security Council (NSC). The National Security Act of 1947 established the National Security Council to advise the President on the integration of domestic, foreign, and military policies relating to national security. The NSC acts as the highest Executive Branch entity providing review of, guidance for, and direction to the conduct of all national foreign intelligence, counterintelligence, special activities, and attendant policies and programs. The NSC, or a committee established by it, considers and submits to the President a policy recommendation, to include dissents, on each special activity, and reviews proposals for other sensitive intelligence operations.

b. Central Intelligence Agency (CIA). The Central Intelligence Agency also was established by the

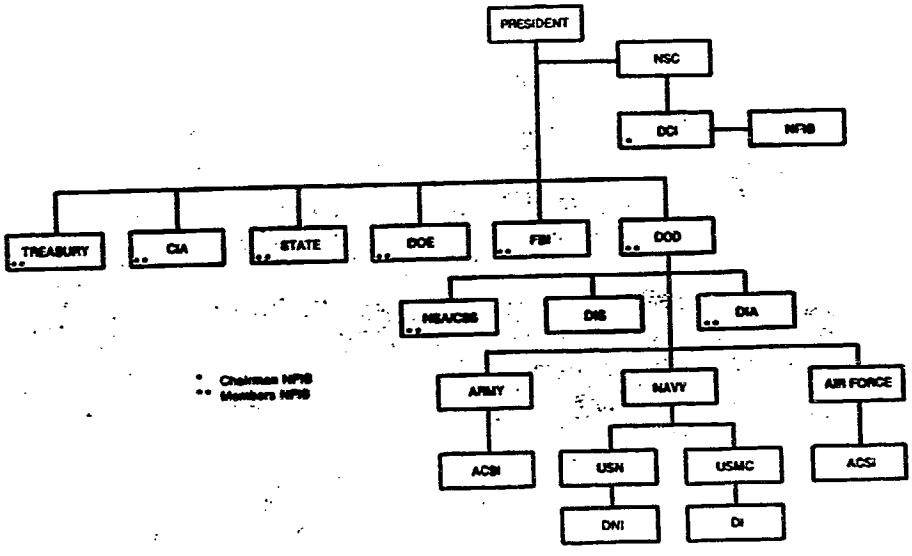


Figure 2-1. Organization for Intelligence.

National Security Act of 1947 and is authorized by: this act, as amended; the CIA Act of 1949, as amended; and other appropriate directives and applicable laws to:

- Collect, produce, and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable. The collection of foreign intelligence or counterintelligence within the United States must be coordinated with the Federal Bureau of Investigation (FBI).

- Collect, produce, and disseminate intelligence on foreign aspects of narcotics production and trafficking.

- Conduct counterintelligence activities outside the United States and, without assuming or performing any internal security functions, conduct counterintelligence activities within the United States in coordination with the FBI.

- Coordinate counterintelligence activities and the collection of information not otherwise obtainable, when conducted outside the United States by other departments and agencies.

- Conduct special activities approved by the President. No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to Congress under the War Powers Resolution) may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective.

- Perform services of common concern for the intelligence community, as directed by the NSC.

- Carry out, or contract for research, development, and procurement of, technical systems and devices relating to authorized functions.

- Protect the security of its installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar association with the CIA as may be necessary.

- Conduct such administrative and technical support activities, within and outside of the United States, as are necessary to perform the functions described above, including procurement and essential cover and proprietary arrangements.

The Director of the CIA also serves as the Director of Central Intelligence (DCI). The DCI is the senior

intelligence advisor to the President, has authority for approval of the National Foreign Intelligence Program budget, and provides the overall coordination, planning, and review of intelligence programs and activities. The National Intelligence Tasking Center (NITC), under direction of the DCI, is responsible for tasking and coordination of national foreign intelligence collection activities. In addition, the DCI is responsible for the protection of intelligence sources and methods from unauthorized disclosure. The DCI also serves as the Chairman of the National Foreign Intelligence Board (NFIB).

c. National Foreign Intelligence Board

(1) The National Foreign Intelligence Board is the focal point for the national intelligence organization and is the primary agency for coordinating intelligence and the intelligence activities of governmental departments. The NFIB is comprised of senior representatives of national foreign intelligence community organizations who are involved in the collection, processing, and production of national intelligence. The membership is as follows:

- Director of Central Intelligence, Chairman.
- Deputy Director of Central Intelligence, Vice Chairman and CIA member.
- Director, National Security Agency.
- Director, Defense Intelligence Agency.
- Director, Intelligence and Research, Department of State.
- Assistant Director, Federal Bureau of Investigation (Intelligence Division).
- Principal Deputy Assistant Secretary for International Affairs, Department of Energy.
- Special Assistant to the Secretary of the Treasury (National Security).
- Appropriate representatives from offices for reconnaissance programs within the Department of Defense will serve as members when programs under their purview are to be discussed; they may attend as observers at other sessions.
- Senior representatives of military intelligence services will attend as observers and may participate at the invitation of the Director of Central Intelligence.

(2) The NFIB is responsible for:

- Production, review, and coordination of national foreign intelligence.
- Interagency exchanges of foreign intelligence information.
- Arrangements with foreign governments on intelligence matters.
- Protection of intelligence sources and methods.
- Activities of common concern to the intelligence community.
- Other matters referred to it by the Director of Central Intelligence.

d. Department of State. The Department of State (Bureau of Intelligence and Research) is responsible for:

- Overtly collecting information relevant to United States foreign policy concerns.
- Producing and disseminating foreign intelligence concerning United States foreign policy, as required, for the execution of the Secretary of State's responsibilities.
- Disseminating, as appropriate, reports received from United States diplomatic and consular posts.
- Transmitting intelligence community report requirements to the Chiefs of United States Missions abroad.
- Supporting Chiefs of U.S. Missions in discharging their statutory responsibilities for direction and coordination of mission activities.

(Note: The Bureau of Intelligence and Research provides intelligence, research, and analysis for the Department of State and other Federal agencies. The Bureau primarily is concerned with political intelligence and produces intelligence studies and current intelligence analysis essential to foreign policy determinations.)

e. Department of the Treasury. The Department of the Treasury is responsible for:

- Overtly collecting foreign financial and monetary information.
- Participating with the Department of State in the overt collection of general foreign economic information.
- Producing and disseminating foreign intelligence concerning United States economic policy, as required, for the execution of the Secretary of the Treasury's responsibilities.
- Conducting activities, through the United States Secret Service, and as authorized by the Secretary of the Treasury or the President, to determine the existence and capability of surveillance equipment used against the President of the United States, the Executive Office of the President, other Secret Service protectees, and United States officials.

f. Department of Energy (DOE). The Department of Energy is responsible for:

- Participating with the Department of State in the overt collection of information on foreign energy matters.
- Producing and disseminating foreign intelligence necessary for discharge of the Secretary's responsibilities.
- Participating in the formulation of intelligence collection and analysis requirements where the special expert capability of the department can contribute.
- Providing expert technical, analytical, and research capability to other agencies within the intelligence community.

g. National Security Agency (NSA). The National Security Agency is responsible for the:

- Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations conducted through other elements of the intelligence community. No other department or agency may engage in signals intelligence activities except when delegated by the Secretary of Defense.
- Control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders.
- Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence.
- Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence.
- Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the government, including the military services in accordance with guidance from the Director of Central Intelligence.
- Collection processing and dissemination of signals intelligence information for counterintelligence purposes.
- Execution of the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government.
- Conduct of research and development to meet the needs of the United States for signals intelligence and communications security.
- Protection of the security of its installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA, as are necessary.

- Security regulations, covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercising the necessary supervisory control to ensure compliance with the regulations.

- Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence.

- Conduct of such administrative and technical support activities, within and outside the United States, as are necessary to perform the functions authorized above, to include procurement.

(Note: The National Security Agency/Central Security Service (CSS) is a separate agency within the Department of Defense and is under the direction and control of the Secretary of Defense. The basic functions of the NSA/CSS include communications security, signals intelligence, and related cryptological activities. The CSS was established under the NSA in 1972 to provide for the centralized management and control of the service cryptologic agencies of the military departments. The Director of the NSA concurrently serves as the Chief of the CSS. Further information is contained in FMFM 2-3, (C) *Signals Intelligence/Electronic Warfare Operations* (U).)

h. Federal Bureau of Investigation (FBI). The Federal Bureau of Investigation, under the supervision of, and pursuant to, the regulations prescribed by the Attorney General, is responsible for:

- Conducting counterintelligence and coordinating counterintelligence activities of other agencies within the intelligence community in the United States. Counterintelligence activity of the FBI involving military or civilian personnel of the Department of Defense shall be coordinated with the Department of Defense.

- Conducting counterintelligence activities outside the United States in coordination with the CIA as required by procedures agreed to by the Director of Central Intelligence and the Attorney General.

- Conducting, within the United States, activities to collect or support foreign intelligence collection requirements of other agencies within the intelligence community or, when requested by the Director of the National Security Agency, supporting the communications security activities of the United States Government.

- Producing and disseminating foreign intelligence and counterintelligence.

- Carrying out or contracting for research development and procurement of technical systems and devices relating to the functions authorized above.

i. Defense Intelligence Agency (DIA) (Department of Defense). The Defense Intelligence Agency was established by a Secretary of Defense directive. The chain of command runs from the Secretary of Defense through the Joint Chiefs of Staff to the Director, DIA. The DIA performs the following functions:

- Develops and produces all DOD intelligence estimates and contributions to national estimates for the National Foreign Intelligence Group.

- Provides for the assembly, integration, and validation of all DOD intelligence requirements and the assignment of relative priorities thereto; assigns specific requirements to DOD collection resources; and originates requests, when necessary, to non-DOD collection resources to fulfill DOD requirements.

- Maintains a single DOD collection requirements registry and facility which is fully compatible with any national requirements registry and facility.

- Provides plans, programs, policies, and procedures for DOD collection activities.

- Provides all DOD current intelligence.

- Conducts coordinating and planning activities to achieve maximum economy and efficiency in the conduct and management of all DOD intelligence activities.

- Provides military intelligence to the Secretary of Defense, staff assistants to the Secretary, military

departments, Joint Chiefs of Staff, specialized DOD agencies, unified and specified commands, and other organizations in the national intelligence community.

- Cooperates with the CIA and other intelligence organizations for mutual support; common and combined usage of facilities, resources, and training programs; and elimination of duplication.
- Manages the Defense Attache System.

j. Defense Investigative Service (DIS). The Defense Investigative Service was established in 1972 as a separate operating agency and is currently under the direction of the Office of the Secretary of Defense (Policy). DIS conducts personnel security investigations (PSI's) for DOD components within the 50 states, the District of Columbia, and the Commonwealth of Puerto Rico. It also investigates unauthorized disclosure of information at the national level within DOD components lacking investigative capabilities and on cases crossing component lines. DIS administers assigned Defense Industrial Security Programs on behalf of the DOD and other federal departments as directed. The Army, Navy, and Air Force investigative organizations assume PSI leads on behalf of the DIS in areas outside the continental United States and are responsible for pursuing investigative matters resulting from PSI's with significant counterintelligence or criminal ramifications. As a central control point for PSI's, the DIS operates the Personnel Security Investigation Center, the National Agency Check Center, and the Defense Central Index of Investigations for DOD components.

203. Military Department and Service Intelligence Organizations

a. Department of the Army

(1) Assistant Chief of Staff for Intelligence (ACSI), Department of the Army. The Assistant Chief of Staff for Intelligence has general staff responsibility for all matters pertaining to intelligence and counterintelligence requirements, and for supervising Army intelligence and counterintelligence collection, production, and dissemination. The ACSI reports directly to the Chief of Staff, U.S. Army.

(2) Army Intelligence and Security Command. The U.S. Army Intelligence and Security Command, under the supervision of the ACSI, is responsible for Army counterintelligence activities in the United States and certain other specified geographic areas. Military intelligence groups (counterintelligence) are the primary operating elements of the intelligence agency with the mission of providing counterintelligence support in specific geographic areas. The military intelligence groups are further organized into regional field offices, and resident offices.

(3) Tactical Counterintelligence Elements. Counterintelligence support to Army tactical units is provided by military intelligence battalions or groups comprising counterintelligence elements as well as by other intelligence specialists. Tactical intelligence units are controlled by the commander of the unit to which they are attached, with general staff supervision exercised by the unit intelligence officer. Additional counterintelligence units may also be assigned to Army support commands for area security.

b. Department of the Air Force

(1) Assistant Chief of Staff, Intelligence. The Assistant Chief of Staff, Intelligence reports directly to the Chief of Staff, U.S. Air Force and has general staff responsibility for matters pertaining to the intelligence activities of the Air Force. The ACSI develops and implements Air Force intelligence plans and policies; coordinates the collection, production, and dissemination of air intelligence; and monitors the worldwide targeting efforts.

(2) **Inspector General (IG).** The Inspector General acts as an advisor to the Chief of Staff, U.S. Air Force and serves as a professional assistant to the Secretary of the Air Force. The Inspector General provides for the investigation of matters within Air Force jurisdiction involving crime, espionage, sabotage, subversion, disaffection, and related matters. The Inspector General also directs the counterintelligence programs within the Air Force and establishes security policy.

(3) **Office of Special Investigation (OSI).** The Office of Special Investigation, under the direction of the Inspector General, provides criminal, counterintelligence, personnel security, and special investigative services to Air Force activities; and collects, analyzes, and reports information concerning these matters.

c. Department of the Navy

(1) **Director of Naval Intelligence (DNI).** The Director of Naval Intelligence exercises overall staff responsibility throughout the Department of the Navy in matters pertaining to intelligence, counterintelligence, and security.

(2) **Naval Intelligence Command (NIC).** Under the command of the Chief of Naval Operations (CNO), the Commander, Naval Intelligence Command (COMNAVINTCOM) commands the Naval Intelligence Command headquarters and those component commands assigned by the Chief of Naval Operations. COMNAVINTCOM's mission is to direct and manage the activities of the Naval Intelligence Command to ensure the fulfillment of the intelligence requirements and responsibilities of the Department of the Navy. The NIC headquarters provides the requisite staff support to the commander in fulfilling his responsibilities with regard to managing intelligence manpower, personnel, and training; intelligence collection, production, and dissemination; intelligence planning, programming, and budgeting; and providing Navy-wide management of the special security officer/special activities officer programs.

(a) The component commands include:

- The Naval Intelligence Support Center (NISC), which analyzes and produces scientific, technical, and current intelligence, and develops threat assessments on foreign naval systems.
- The Naval Field Operational Intelligence Office (NFOI), which produces finished operational intelligence, ocean surveillance information, and indications and warning.
- The Naval Intelligence Processing Systems Support Activity (NIPSSA), which plans and manages naval intelligence information processing and communication systems.

(b) The Naval Investigative Service (NIS), formerly a component command, became a second echelon command in September 1981; therefore, the Naval Intelligence Command no longer has investigative or counterintelligence responsibilities.

(3) **Naval Investigative Service (NIS).** The Director of the Naval Investigative Service maintains a worldwide organization composed of Navy and Marine Corps personnel responsive to command requirements of both Services. In addition to the investigation of major criminal offenses, the NIS is responsible for counterintelligence investigations and operations, except those combat-related counterintelligence matters within the functional responsibilities of the Marine Corps. (See par. 103g.) During combat or in a combat contingency environment, the commander amphibious task force (CATF) and the commander landing force (CLF) ashore exercise immediate control over assigned Navy and Marine Corps investigative and counterintelligence assets. In addition to regularly assigned Marine Corps counterintelligence personnel, NIS may also be provided with counterintelligence personnel from FMF commands during peacetime in accordance with a Service agreement between the Commandant of the Marine Corps (CMC) and the Director of NIS. Further details on the jurisdiction and responsibilities of NIS are contained in SECNAV Instruction 5520.3__.

(4) Director of Intelligence, Headquarters, U.S. Marine Corps. The Director of Intelligence, Headquarters, U.S. Marine Corps, is responsible to the Commandant of the Marine Corps for the formulation of plans and policies pertaining to intelligence and counterintelligence within the Marine Corps. The Head, Counterintelligence Branch is the principle advisor to the Director of Intelligence for counterintelligence matters. The Counterintelligence Branch performs the following functions:

- Prepares counterintelligence plans, policies, and directives.
- Formulates counterintelligence doctrine and missions.
- Coordinates with national level government agencies.
- Acts as counterintelligence military occupational specialty (MOS) sponsor.
- Maintains staff cognizance over counterintelligence field units and staff management of training.
- Exercises staff responsibility for human intelligence (HUMINT) resources and certain classified programs.
- Coordinates with the Naval Investigative Service (NIS) in special investigations and operations.
- Provides for the evaluation and procurement of specialized equipment.
- Conducts security reviews.
- Reviews reports from the field commands concerning security violations, loss of classified material, and compromises.
- Coordinates the release of information for foreign disclosure.
- Provides representatives to national level counterintelligence and security committees.

204. Fleet Marine Force Counterintelligence Organization

a. Staff Counterintelligence Officer

(1) The staff counterintelligence officer is an integral part of the intelligence staff of FMF headquarters, Marine amphibious forces (MAF's), divisions, and aircraft wings. The staff counterintelligence officer advises and assists the assistant chief of staff, G-2 in carrying out the command's counterintelligence responsibilities and is the focal point for the coordination of the counterintelligence effort.

(2) The staff counterintelligence officer performs the following functions:

- Assists and advises the G-2 in the formulation, interpretation, and implementation of counterintelligence policy.
- Coordinates counterintelligence services provided to the command.
- Serves as the principal point of contact between the command and the NIS in matters involving the investigation of actual, potential, or suspected espionage, sabotage, terrorism, and subversive activities, including defection, ensuring that information about these activities is reported promptly to the nearest Naval Investigative Service representative.
- Maintains liaison with the NIS and other counterintelligence agencies.
- Monitors the command counterintelligence and security training program and provides advice and assistance for the maintenance of an effective program.
- In coordination with the communication officer and other staff officers, advises in the maintenance of the physical security aspects of communications security.

(3) The staff counterintelligence officer performs the following operational functions:

- Prepares counterintelligence directives, plans, reports, and estimates, including portions of estimates, reports, and studies prepared under the supervision of other G-2 elements.
- Plans, implements, and supervises all active and passive counterintelligence measures within the command.
- Coordinates counterintelligence measures, operations, and activities with lower, adjacent, and higher headquarters.
- Provides counterintelligence advice and input to contingency operation plans for training exercises.
- Maintains counterintelligence reference material for contingency planning and provides for further dissemination as appropriate.
- Serves as a member of the command's operations security (OPSEC) committee, where such committees exist.
- Plans, implements, and coordinates the collection of information through special operations and the use of human intelligence resources during combat operations.
- Conducts planning for the intelligence and counterintelligence processing of friendly prisoners of war who have been returned to friendly control.

(4) The primary efforts of the staff counterintelligence officer are directed toward planning and coordinating combat counterintelligence operations and ensuring that assigned or attached counterintelligence teams are employed properly. Counterintelligence planning must be incorporated into all contingency operation plans to ensure effective employment of counterintelligence assets and proper security of operational elements. During training exercises, counterintelligence planning is accomplished as early as possible and provides for the realistic training of counterintelligence personnel.

(5) The staff counterintelligence officer serves as the headquarter's counterintelligence advisor and monitors the overall command counterintelligence program. Counterintelligence personnel will not perform routine administrative duties associated with the information security program, including processing security clearances, maintaining command access programs, and maintaining the unit's or command's classified files. These tasks are the functional responsibility of the command administrative personnel; assistant chief of staff, G-1; and the command security manager. The staff counterintelligence officer coordinates counterintelligence services and makes recommendations to the security manager on the adjudication of security investigations, violations, and compromises.

(6) The staff counterintelligence officer is responsible for recommending to the assistant chief of staff, G-2 the mission, tasks, and responsibilities of the assigned or attached counterintelligence team(s). The staff counterintelligence officer coordinates and supervises the overall counterintelligence effort and tasking of assigned or attached counterintelligence teams(s). The relationship of the staff counterintelligence officer and the team commander is similar to that of a staff officer and the commander of a subordinate unit. The team commander should be permitted to deploy the team in a manner best suited to accomplish his assigned mission and tasks.

(7) At the Marine amphibious force (MAF) level, the staff counterintelligence officer must monitor all counterintelligence activity within the MAF, including that of detached counterintelligence teams or subteams, to ensure that MAF counterintelligence objectives are accomplished. Accordingly, close coordination of all counterintelligence activities must be accomplished among all staff counterintelligence officers at all levels of command.

(8) In order to ensure comprehensive, all-source counterintelligence estimates and views are available to the supported commander, the staff counterintelligence officer must possess access to appropriate compartmented intelligence material.

b. Counterintelligence Teams

(1) Counterintelligence teams are combat support elements, organic to the MAF, organized and equipped under tables of organization and equipment of the 4722 series. As intelligence specialist teams, they are assigned to the assistant chief of staff, G-2 to accomplish specific counterintelligence objectives. The assistant chief of staff, G-2 exercises direction, control, and supervision of the teams through the staff counterintelligence officer.

(2) Counterintelligence teams are assigned to major FMF commands. Three teams are normally assigned to each MAF and one team each to the Headquarters, Fleet Marine Force Pacific (FMFPAC) and Fleet Marine Force Atlantic (FMFLANT). The control and coordination of counterintelligence teams at the MAF level is essential to ensure an economical, flexible, and coordinated response to the enemy intelligence threat within the MAF area of responsibility. Garrison counterintelligence team attachments will be the responsibility of the respective FMF headquarters and will be coordinated with the Commandant of the Marine Corps.

(3) Counterintelligence teams assigned to the MAF are normally retained in a general support role under the centralized control of the MAF. In cases where units are widely separated, operations would be facilitated, or units are deployed separately; counterintelligence teams may be further attached to divisions, aircraft wings, or Marine amphibious brigades (MAB's). When commands of less than division, aircraft wing, or MAB size require direct counterintelligence support, attachment of counterintelligence subteams is appropriate. The MAF counterintelligence organization is shown in figure 2-2. Counterintelligence

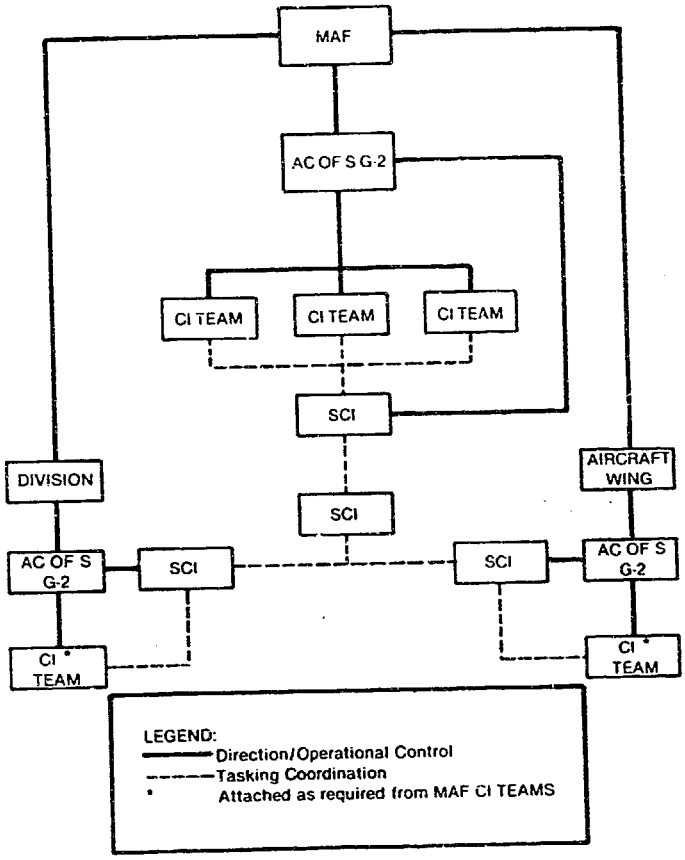


Figure 2-2. Marine Amphibious Force Counterintelligence Organization.

support for these units is normally provided by the MAGTF headquarters counterintelligence teams or by locally assigned counterintelligence assets. Counterintelligence subteams or teams (as appropriate to the operational environment) may be assigned by the FMF/MAF commander to the force service support group (FSSG) when the FSSG cannot be supported by the division, aircraft wing, or Marine air-ground task force (MAGTF) counterintelligence assets and requires direct counterintelligence support.

(4) Counterintelligence teams assigned to Headquarters, FMFPAC and FMFLANT provide the commander with the means to meet specific operational requirements and provide support to areas where gaps in counterintelligence coverage may exist due to deployment of MAF commands.

(5) The standard counterintelligence team consists of five officers, nine enlisted counterintelligence specialists, and two administrative clerks. The team is organized into a team headquarters and four subteams, each consisting of one officer and two counterintelligence specialists. The counterintelligence team is based on a modular concept permitting the task organization of a team by the attachment or detachment of subteams as required. The standard counterintelligence team organization is shown in figure 2-3.

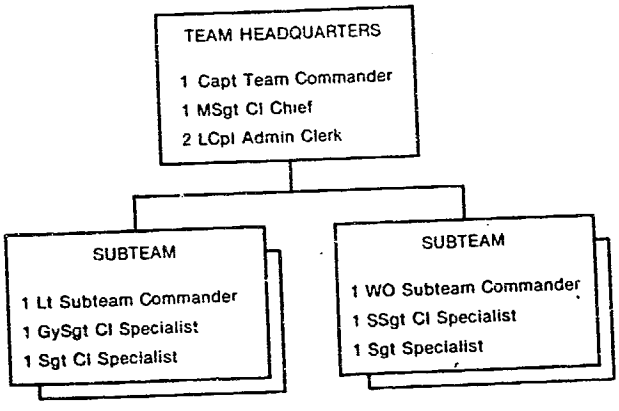


Figure 2-3. Standard Counterintelligence Team.

(6) Counterintelligence teams are equipped for tactical operations and maintain sufficient organic equipment to support the team headquarters and the separate deployment of fully equipped subteams. The team is not capable of self-administration and requires administrative and logistics support from the unit to which assigned or attached. Equipment authorized by counterintelligence teams' tables of equipment, however, remains organic to the counterintelligence team regardless of supply and maintenance assistance and support.

(7) Counterintelligence teams operate under the staff cognizance of the assistant chief of staff, G-2 and perform the following functions as directed:

- Conduct active and passive counterintelligence operations including counterespionage, countersubversion, counterterrorism, and counter sabotage in support of tactical units during combat operations.
- Conduct intelligence collection operations utilizing human intelligence sources during combat operations.
- Conduct counterintelligence investigations pertaining to espionage, sabotage, terrorism, and subversion, including defection and other special counterintelligence investigations as required during combat operations.
- Assist the staff counterintelligence officer in the preparation of counterintelligence estimates and plans for areas of operation reflected by contingency plans.
- Participate in field training exercises of Marine amphibious units (MAU's) or larger commands. Participation in exercises of smaller units is appropriate provided realistic and meaningful counterintelligence activities can be developed. Participation should include assignment of counterintelligence personnel to the exercise planning staff to ensure adequate counterintelligence activity in the exercise.
- Maintain information concerning personalities, organizations, and installations of

counterintelligence interest which support combat contingency plans.

- Conduct counterintelligence surveys of commands and installations to determine the security measures necessary to provide protection against espionage, sabotage, subversion, and terrorism and the unauthorized disclosure of, or access to, classified material.

- Conduct counterintelligence evaluations and inspections of areas containing classified material.

- Conduct technical surveillance countermeasures (TSCM) inspections and surveys of sensitive areas in accordance with MCO 05511.11__. These inspections and surveys are conducted by a designated counterintelligence team within each MAF, which has a TSCM capability.

- Preparation and conduct of penetration inspections to test the counterintelligence and security measures of the command. These inspections may be in conjunction with the OPSEC program where appropriate. Counterintelligence assets should direct their efforts towards identification of friendly vulnerabilities which can be exploited by hostile collection assets and recommend appropriate countermeasures to the command OPSEC officer.

- Provide instructors in counterintelligence and security subjects for the command training program. (Section 6 provides details on counterintelligence and security subjects for command training programs.)

- During combat operations, collect and maintain information designed to identify, locate, and recover friendly personnel captured, missing (nonhostile), and missing in action.

- Conduct the intelligence and counterintelligence debriefing of friendly prisoners of war who are returned to U.S. control.

- Conduct liaison with unit intelligence sections and local intelligence, counterintelligence, and law enforcement agencies as appropriate.

(8) Counterintelligence interest in physical security will often overlap with the functional responsibilities of the provost marshal. During the conduct of counterintelligence surveys, counterintelligence personnel are concerned with physical security as it relates to all aspects of counterintelligence, while in the case of counterintelligence evaluations and inspections, this interest primarily is directed toward the protection of classified material. Concurrently, functional interests of the provost marshal/military police are physical security measures designed to safeguard personnel; prevention of unauthorized access to equipment, facilities, material, and documents; and the safeguarding of them against espionage, sabotage, terrorism, damage, and theft. The overlapping physical security interests, equally applicable in garrison and combat, must be effectively coordinated to ensure optimum security of the command. Counterintelligence personnel may not be utilized to assess physical security areas unrelated to counterintelligence, such as armories, post exchanges, disbursing offices, and clubs, where the security thrust is the prevention of damage, theft, and/or pilferage. This function is under the cognizance of the provost marshal.

(9) Counterintelligence assets should not be utilized to perform functions such as criminal investigations or incident reporting which would more appropriately come under the cognizance of other assets available to the commander.

205. Marine Corps Supporting Establishment Counterintelligence Personnel

Counterintelligence personnel are assigned to major Marine Corps bases and support activities to advise and assist in planning and implementing the command counterintelligence effort.

Counterintelligence personnel assigned to the supporting establishment perform nontactical counterintelligence functions normally performed by FMF staff counterintelligence officers and counterintelligence teams.

206. Commands Without Assigned Counterintelligence Personnel

Commands that do not have counterintelligence personnel assigned or attached, are still responsible for establishing counterintelligence measures to ensure the security of the command and to deny the enemy, information which might be used to increase the effectiveness of hostile operations against the command. These commands, however, conduct neither counterintelligence investigations, nor special operations against enemy capabilities in the fields of espionage, sabotage, subversion, or terrorism. If these types of investigations or operations appear to be required, a request must be submitted to the local Naval Investigative Service office. When appropriate, the request should go through the chain of command for concurrence of the commander who has counterintelligence staff advisors.

Those commands not assigned or attached counterintelligence personnel normally operate as part of larger commands having counterintelligence personnel. These counterintelligence specialists are usually available, upon request, to provide advice and assistance on such matters as conducting lectures and demonstrations, testing unit security, advising on counterintelligence measures to be adopted, and checking security of offices, war rooms, and other areas used for the preparation or stowage of classified material.

207. Liaison

Effective performance in the field of counterintelligence requires extensive liaison. Counterinteligence activities often closely parallel functions and responsibilities of other organizations and agencies and, in some cases, may overlap. Close and continuous liaison and coordination aids in the effectiveness of operations, the exchange of information, and in providing for mutual assistance.

Policies and procedures for liaison and the coordination of counterintelligence activities are developed and promulgated at the general staff level. Depending on the area of operations and the type of counterintelligence activity, liaison and coordination is normally conducted by counterintelligence elements with local intelligence, counterintelligence, security and law enforcement organizations/agencies, and civil affairs and psychological operations units where appropriate. In all cases, liaison must be conducted within jurisdictional limitations imposed by higher authority.

Section 3

Counterintelligence Combat Operations

301. General

Major Fleet Marine Force (FMF) units are provided counterintelligence support by assigned or attached counterintelligence teams. During tactical operations, counterintelligence activities are characterized by aggressive, resourceful, and well-coordinated operations designed to protect the command from hostile intelligence collection, sabotage, terrorism, and subversive activities. Counterintelligence teams contribute to mission accomplishment by assisting the commander in accomplishing his counterintelligence responsibilities.

302. Counterintelligence Mission

The mission of counterintelligence assets in Fleet Marine Force units is to plan and recommend the implementation of measures designed to discover, neutralize, or destroy the effectiveness of actual or potential hostile intelligence, sabotage, terrorist, and subversive activities, and to recommend measures necessary for the protection of information against espionage, personnel against subversion and terrorism, and installations and materiel against sabotage.

303. Categories of Counterintelligence Operations

Counterintelligence operations within the Fleet Marine Forces normally comprise the following five categories:

a. Military Security. Military security encompasses all measures taken by a command to protect itself from sabotage, terrorism, and subversion, and to deny information to the enemy. In Fleet Marine Force units, it emphasizes protection of airfields and other

major installations, and the defeat of hostile target acquisition efforts. Typical measures include operations security (OPSEC), counterreconnaissance, countersigns, passwords, and restrictions on access to selected areas and installations.

(1) Operations Security

(a) OPSEC denies the enemy prior knowledge of essential elements of friendly information (EEFI) regarding command activities, plans, operations, and intentions. The enemy collects this information through a variety of means. To effectively counter this threat, commanders must have access to reliable information on enemy intelligence capabilities. This information must be timely and accurate to ensure commanders maximum security for their operations.

(b) Counterintelligence units support the commanders' OPSEC programs by providing assessments of friendly vulnerabilities; briefings on enemy threats of espionage, sabotage, subversion, and terrorism; and assistance in establishing safeguards against those security threats.

(c) OPSEC is the functional responsibility of the operations officer (G-3/S-3). To be effective, OPSEC principles and concepts must be established and continuously practiced during the conduct of peacetime operations as well as in combat environments. Commanders, staffs, and individuals at all echelons of command are responsible for developing an effective OPSEC program. Commanders must determine what OPSEC measures to implement, when to implement them, and what level of risk they are willing to accept.

(d) An OPSEC committee should be formed at each command consisting of the following staff sections: G-3 (Chairman), G-2, G-4, G-1, public affairs, communications-electronics, adjutant, medical, and others as desired. The committee is responsible for the overall planning and monitoring of the OPSEC program. Commanders should ensure that OPSEC is considered in the initial planning phase of all operations. The OPSEC plan should include, as a minimum, the EEFI for the operation and should state specific countermeasures which will be implemented to enhance surprise and increase security for the command operation. OPSEC concepts and techniques should be developed to include the following:

1 **Central Control and Direction.** This may be accomplished through the establishment of an OPSEC team comprised of members of the operations section (G-3/S-3), intelligence section (G-2/S-2), and communications-electronics section. Through assets available to them (counterintelligence, signals intelligence, photoimagery interpretation, etc.), the OPSEC team will direct its efforts towards the identification of enemy intelligence collection assets and recommending countermeasures, including the use of deception.

2 **Close Integration of Operations, Communications Security, and Counterintelligence.** Members of the OPSEC team will review and monitor operation plans, actions, and after-action reports for evidence of indicators which disclose EEFI, establish patterns, or provide other mission-oriented information to the enemy. Continuous efforts will be maintained to discover enemy methods of information collection directed towards the command. Upon discovery of such indicators and/or methods, recommended methods of improving friendly security and/or nullifying the enemy's collection capabilities will be provided to the commanders.

3 **Operations Security Data Base.** The OPSEC officer is responsible for developing and maintaining an OPSEC data base. As information is developed on friendly vulnerabilities and enemy intelligence capabilities, it is analyzed, acted on, and filed in an easily retrievable manner. The information, especially that concerning enemy intelligence capabilities, is continually updated and used to plan methods of information denial and/or deception. The type information that might be found in the data base is as follows:

- Unit communication equipment/procedures.
- Communication violations.
- Counterintelligence measures in effect.
- Imagery of friendly positions.

- Technical collection and operational capabilities of known enemy units in the area of operations, including operational capabilities of equipment.
- Enemy sightings/contacts.
- Clandestine enemy personnel, organizations, and installations.
- Record of camouflage/blackout discipline.

(2) Counterreconnaissance. Of all the counterintelligence measures that are taken by a unit in combat, one of the most effective is counterreconnaissance. Units may be assigned both reconnaissance and counterreconnaissance responsibilities; these two activities complement each other and are inseparable. Good reconnaissance ensures a certain amount of security, and counterreconnaissance provides a certain amount of reconnaissance information; however, a unit armed and equipped for a pure reconnaissance mission is not ordinarily given a supplementary counterreconnaissance mission as accomplishment of the counterreconnaissance mission generally requires defeat of hostile reconnaissance elements. The primary object of reconnaissance is collection of information, not combat. Counterintelligence includes all measures taken to prevent hostile observation of a force, area, or place. Counterreconnaissance can include the setting up of a defensive screen to deny enemy reconnaissance or an offensive screen designed to meet and destroy enemy reconnaissance. In combat air operations, counterair operations to deny or reduce an enemy's capability for visual, photographic, or electromagnetic reconnaissance may be defined as counterreconnaissance.

(a) Principles of Counterreconnaissance. Counterreconnaissance elements focus on friendly forces being screened; hostile reconnaissance forces are destroyed or neutralized by combat, and friendly screening forces are echeloned in depth.

(b) Forms of Counterreconnaissance

1 The defensive screen is protective and is usually established behind natural obstacles.

2 The offensive screen meets the enemy's reconnaissance forces and destroys them. An offensive screen may be moving or stationary depending on the activities of the friendly force being screened.

3 The commander's adoption of a form of counterreconnaissance screen is dependent upon the situation, mission, weather, and terrain; thus the form of counterreconnaissance screen adopted need not reflect solely the tactical mission of the command. The fact that there are offensive and defensive screens does not imply a requirement for their employment only in support of a like tactical mission. An offensive screen may well be employed to support a tactical mission of defense, while an attack mission may be supported best by a defensive screen.

(3) Countersigns

(a) Dissemination

1 Countersigns, each consisting of a challenge and password, are normally issued as a tab to the counterintelligence appendix to the intelligence annex to the operation order. They appear as shown in the following examples:

Identifying Code Number	Challenge	Password
11	Lamp	Wheel
12	Powder	Quaint
13	Glass	Table

2 Words that are closely associated or normally used in conjunction with one another are avoided. Unless compromised or otherwise changed, countersigns are normally effective for no more than 24 hours. Dissemination of the initial primary and alternate countersign for the first period troops are ashore can be made in the counterintelligence appendix to the intelligence annex. Subsequent countersigns can be disseminated in a message such as the following: *Code 11 countersign effective 012300 (local time), alternate code 13.*

(b) Compromise. When a unit knows or suspects that the designated countersign has been compromised, the alternate is put into effect by that unit. Landing force headquarters must be immediately notified so that subordinate and adjacent units can be informed that the alternate countersign is in effect and a new alternate countersign is then designated.

(c) Use of the Countersign. It must be emphasized that countersigns are not used when other means of identification are possible. Further, neither the challenge nor the password is given in a loud voice.

b. Civil Security. Civil security operations include all the counterintelligence measures affecting the population of the area. Typical measures include security screening of civilian labor, imposition of curfews, other circulation control measures, and the monitoring of suspect political groups.

c. Embarkation Security. Embarkation security consists of the special application of military and civil security measures to the embarkation phase, which includes the movement to the point of embarkation and the actual embarkation. Examples include the screening of civilians employed in the port or airfield, control of contact between troops and civilians, covering or removing tactical markings and other unit designations, and moving to the port or airfield under cover of darkness.

d. Wartime Information Security Program (WISP). The Wartime Information Security Program is the control and examination of communications to prevent disclosure of information of value to an enemy and the collection of information of value to the United States.

e. Special Operations. Special counterintelligence operations include the specialized employment of active and deceptive counterintelligence techniques and procedures in the conduct of covert operations against hostile and unfriendly intelligence collection, sabotage, terrorism, and subversive organizations and activities. These operations are conducted by trained counterintelligence personnel and include the following:

(1) Counterespionage. Counterespionage operations are designed to detect or expose hostile espionage efforts and to institute offensive measures intended to penetrate and nullify hostile intelligence plans and operations, thus contributing to the security of the FMF in the field.

(2) Countersubversion. Countersubversion operations are designed to detect, prevent, or neutralize the activities of subversive groups. Because subversive activity is closely related to and frequently supports, conceals, or provides a favorable environment for hostile espionage and sabotage operations, the countersubversive mission may include offensive measures directed toward the origin of hostile subversive plans and policies.

(3) Countersabotage. Countersabotage operations require a comprehensive program of defensive measures and aggressive offensive action to penetrate saboteur, partisan, or other dissident groups to determine sabotage plans, and to identify saboteurs, methods of operation, and specific targets. Sabotage is a principal weapon of guerrilla and partisan groups, and is increasingly important as a threat to rear area logistics installations.

(4) Counterterrorism. Counterterrorism operations are designed to detect, restrain, or neutralize those terrorist organizations and personalities who pose a threat to U.S. installations and personnel, or other interest. Counterterrorism operations will be conducted in the same manner as other special operations and will include the collection and analysis of information pertaining to the terrorist threat. (The term antiterrorism refers to the defensive measures by DOD to reduce the vulnerability of DOD personnel and their dependent facilities and equipment to terrorist acts. Antiterrorism measures should not be confused with counterterrorism operations).

304. Forward Area Operations

a. Offensive Operations

(1) Counterintelligence operations during the attack consist primarily of neutralizing, exploiting, or destroying counterintelligence targets which are known to be located in the enemy held areas. These targets are normally contained in the counterintelligence target reduction plan (see par. 504).

(2) Counterintelligence personnel may be deployed with forward elements depending on the number and criticality of identified counterintelligence targets within the objective area. In some instances, it is advantageous for counterintelligence personnel to take immediate custody of persons of counterintelligence interest, while in the case of installations, exploitation may be delayed until forward elements have occupied or passed through the objective area. The preservation and protection of installations of counterintelligence interest, pending exploitation by counterintelligence personnel, is arranged with commanders of lead units.

(3) Flexibility of operations is required to ensure coverage of all counterintelligence targets. Counterintelligence personnel may be deployed from one unit to another and from rear areas to forward elements as the situation changes.

b. Defensive Operations

(1) In the defense, counterintelligence efforts are primarily directed against the enemy intelligence efforts to collect information concerning FMF units, infiltration of enemy intelligence agents, sabotage, and terrorist activities. In a static situation, the enemy can be expected to increase all of these activities, as well as to increase guerrilla force operations against installations, command posts (CP's), lines of communications, supply, and other critical areas.

(2) Counterintelligence elements are normally deployed with the command headquarters rather than forward tactical elements in order to provide timely support to those areas where enemy intelligence activities require a greater counterintelligence effort.

(3) A defensive situation allows for greater development and exploitation of counterintelligence targets. Counterintelligence elements normally accomplish the following:

- Develop an effective human source collection system targeted against enemy intelligence activities.
- Conduct operations against enemy intelligence organizations and activities.
- Screen and interrogate those civilians and prisoners of war who are known to be, or suspected to be, of possible counterintelligence interest.
- Provide security services to enhance the security of critical installations and activities.
- Conduct briefings for the command and other organizations, such as military police, psychological operations units, and civil affairs units, on hostile intelligence activity and methods of operation.
- Conduct counterintelligence investigations as required.
- Conduct investigations and collect information to aid in identifying, locating, and recovering friendly personnel captured, missing (non-hostile), and missing in action.

(4) During a defensive situation, counterintelligence elements may also initiate human intelligence (HUMINT) resources collection programs if the counterintelligence situation permits and the resources are available. These programs are designed to collect order of battle (OOB) information and information concerning enemy intentions. Additionally, counterintelligence units may participate in

certain special operations concerning infiltration of sources, deceptive operations, and exploitation of enemy intelligence agents as directed by higher headquarters.

c. Retrograde Operations

(1) During retrograde operations, the security of troop movements and lines of communications are of prime importance to the commander. Counterintelligence operations and the collection of information must be compatible with the commander's courses of action and designed to limit the effectiveness of enemy intelligence activities during the movement.

(2) Counterintelligence units are normally concerned with the following functions during a retrograde operation:

- Collecting information on enemy intelligence activities that could hinder friendly troop movement.
- Maintaining continuous liaison with military police and other security forces responsible for the control of refugees and other civilians in order to detect persons of possible counterintelligence interest.
- In support of units involved, assisting in and coordinating the inspection of vacated command post areas to ensure that no information or material has been left behind which might benefit enemy forces.
- Evaluating personnel of counterintelligence interest for evacuation and/or protection.
- Evaluating sources of information for evacuation or further operational employment.
- Coordinating activities with counterintelligence and security units of higher and adjacent commands.

305. Rear Area Operations

Those areas in which combat service support (CSS) activities are accomplished are referred to as rear areas. These areas provide a lucrative target for enemy intelligence activity and guerrilla operations. Enemy espionage, sabotage, terrorist, and subversive activities, and the disruption of lines of communications within rear areas may serve to jeopardize combat operations.

Counterintelligence support for rear areas is normally provided by the counterintelligence team supporting the Marine air-ground task force (MAGTF) headquarters. Counterintelligence activities in support of rear area security include the following:

- Collecting information concerning hostile intelligence personalities, organizations, and activities in rear areas.
- Conducting operations to destroy, neutralize, or exploit hostile intelligence elements.
- Developing HUMINT programs.
- Providing security services, including technical surveillance countermeasures (TSCM) support to enhance the security of commands.
- Conducting counterintelligence investigations as required.
- Screening and interrogating those civilians and prisoners of war who are known to be, or are suspected to be, of counterintelligence interest.
- Conducting further exploitation of counterintelligence targets referred from forward tactical commands.
- Providing assistance in and support for the command security orientation and indoctrination program.
- Conducting briefings for unit and installation commanders on the hostile intelligence threat and providing recommendations to enhance security measures.
- Conducting investigations and collecting information to aid in identifying, locating, and recovering friendly personnel captured, missing (nonhostile), and missing in action.

306. Employment of Counterintelligence Teams

a. Operational Concept

(1) Counterintelligence teams are normally assigned to the MAGTF and provide general support within the MAGTF area of operations. Control of counterintelligence teams by the force commander provides the commander with the means to meet the specific operational requirements of various commands within the force and to hold counterintelligence teams or subteams at force level to effect counterintelligence support of subordinate commands as required. In some instances, due to the time element, tactical conditions, or operational exigencies, it may be necessary for the force commander to attach some or all counterintelligence teams to his subordinate tactical commands.

(2) Counterintelligence teams are not normally placed under the operational control of commands of less than Marine amphibious brigade (MAB) size. However, in the case of a landing force of less than MAB size, assignment of subteams is appropriate. In addition, under those circumstances where attachment of subteams to an infantry regiment or aircraft group would facilitate the early reduction of specific counterintelligence targets, attachment of counterintelligence personnel to those units may be appropriate.

(3) During operations involving widely separated units in areas of dense population, counterintelligence subteams may be made available to the unit commanders to accomplish specific counterintelligence missions assigned by higher headquarters.

(4) The tactical concept of operations in depth governs the execution of counterintelligence plans and operations. Counterintelligence teams can be deployed on an area coverage concept or by unit assignment.

(a) **Area Coverage**

1 Counterintelligence teams deployed for area coverage are assigned a specific geographic area of responsibility and provide counterintelligence support to commands located within that area. The team continues to operate within the assigned area even though the tactical or support units operating in the area change.

2 The area coverage concept allows counterintelligence operations to focus on the enemy's intelligence organization and activities while remaining unfragmented and unrestricted by the tactical areas of responsibility assigned to supported units. Area coverage provides the greatest continuity of counterintelligence operations and allows counterintelligence personnel to become thoroughly familiar with the area, enemy intelligence organization and operations, and counterintelligence targets.

3 Area coverage is particularly effective during counterinsurgency operations where the insurgent prefers to operate on the political or military boundaries.

(b) **Unit Assignment.** Counterintelligence teams deployed on a unit assignment basis normally remain with the supported unit and operate within that unit's area of responsibility. As tactical units displace, it is necessary for higher echelons to provide counterintelligence coverage for the areas vacated. Relief of an area can be accomplished in the following manner:

1 **Augmentation Subteams.** Augmentation subteams may be attached from the force level to assault units, in advance of operations, to provide adequate personnel for reduction of specific counterintelligence targets during the initial phases of the operation and to prepare for the transfer of areas of responsibility from assault units to force without loss of continuity. These subteams operate under the direct control of the assault unit during the reduction of

counterintelligence targets and then remain in place as the unit advances, thereby ensuring continuous coverage as the force moves forward and assumes control of the area.

2 **Leapfrog System.** This method requires the team initially responsible for an area to be detached from the assault unit and a new team attached. The new team is attached sufficiently in advance to permit the team to become thoroughly familiar with current operations. This method of relief permits the team familiar with the area, informants, and targets to remain and conduct more extensive operations and is similar to the area coverage concept but on a smaller scale.

3 **Relay System.** This method requires force counterintelligence teams to be held in reserve and dispatched forward to assume control of areas as the assault units move forward.

b. Factors Bearing on the Employment of Counterintelligence Teams

(1) The characteristics of an objective area determine the character and extent of counterintelligence operations required within that area. The density of the population, its cultural level, the attitude of the people and political groups toward friendly and enemy forces and their susceptibility to enemy penetration (hostile intelligence threat) and propaganda, and the stability of local governments are all factors in determining the number of counterintelligence teams needed to accomplish the counterintelligence mission.

(2) The number of counterintelligence teams available has a significant bearing on the ultimate accomplishment of the counterintelligence mission. Overestimation of the teams' capabilities will result in dispersion of activity on many targets with limited effectiveness. Careful planning and a grasp of the overall counterintelligence pattern of operations from rear to forward areas, plus detailed detailed preparation, is required. The counterintelligence targets which, in the overall counterintelligence picture, require early reduction can then be selected and the employment of teams planned.

(3) The commander landing force (CLF), once established ashore, assumes immediate control over all assigned counterintelligence assets. In some instances, Naval Investigative Service (NIS) elements may be assigned in support of the landing force. In such cases, jurisdiction and responsibility must be clearly defined for efficient utilization of counterintelligence assets. Normally, Marine counterintelligence teams are assigned responsibility for counterintelligence operations and investigations which directly support tactical units. Counterintelligence operations and investigations of a general support nature in rear areas are more compatible with the Naval Investigative Service's organization and mission.

c. Employment of Counterintelligence Teams at Division Level

(1) The relative number of personnel devoted to counterintelligence is, as a rule, greater in the Marine division zone of action than in support areas. The constant contact of opposing ground forces and the presence of indigenous or displaced populations in the combat or occupied areas afford the enemy a better opportunity to penetrate the counterintelligence screen. The counterintelligence team operating with a division is usually in the position of being the first security unit to enter territory recently cleared of the enemy. Its role in counterintelligence operations is of primary importance in laying the groundwork for all later security measures. The team secures the most obvious targets, the agents left behind by the enemy for espionage and sabotage, the best known collaborators with the enemy, and key public buildings such as the seat of the local government and the communication centers. Prompt action by a counterintelligence team is often of great value to the security of friendly forces and can make

available, through interrogations and seized documents, important elements of tactical intelligence.

(2) The counterintelligence team normally confines its activities to the area roughly forward of the division command post. Responsibility for rear areas must be assumed by higher echelons. Counterintelligence teams operating with a division are generally deployed by subteams which are responsible for the counterintelligence coverage of specific areas within the jurisdiction of the command. Each subteam acts as an independent unit, but its activities are coordinated by the team commander, who maintains his headquarters near the division command post.

(3) Time is of the essence during the assault phase of an operation. Counterintelligence teams employed with an assault division will generally limit their screening operations to the identification and classification of civilians disguised as military personnel, enemy agents, and collaborators. Although immediate tactical interrogations may be conducted, providing time permits, normally suspects will be passed to rear areas for more detailed interrogations and classification. (Also see par. 307b.)

d. Employment of Counterintelligence Teams at Aircraft Wing Level

(1) There is no significant difference in the mission of counterintelligence teams employed with either ground or air units; however, employment with air units is normally characterized by a static situation.

(2) An aircraft wing is sometimes widely dispersed with each aircraft group operating from a separate field, and wing headquarters operating ashore with the landing force. Since wing equipment is highly susceptible to damage and difficult to replace, wing units are a high priority target for enemy sabotage and terrorism. In most instances, air units have a requirement for the employment of large numbers of indigenous personnel who become a source for enemy intelligence activities. Under these conditions, it may be necessary to provide subteams to Marine aircraft groups (MAG's) or independent squadrons.

(3) In air operations or an airborne movement, counterintelligence personnel are included in the advance command echelon to advise the commander on the control and security of sensitive areas, civilian control measures, screening of local residents and transients, and to check establishments in the vicinity as may be required.

e. Employment of Counterintelligence Teams at Marine Air-Ground Task Force Level

(1) A counterintelligence team supporting the MAGTF headquarters normally operates in the rear areas. Generally, the MAGTF headquarters team completes and follows up on all matters of counterintelligence interest initiated by assault units, conducts special operations of a relatively long-term nature, and provides assistance on military and civil security matters. The MAGTF headquarters counterintelligence team normally has the capability to perform technical surveillance countermeasures inspections and surveys for the entire MAGTF and will establish and operate the MAGTF counterintelligence interrogation center if required. Paragraph 305 details the functions appropriate for counterintelligence support in rear areas.

(2) Within rear areas, two organizations requiring counterintelligence support are the CSS organization and the civil affairs unit. The former is primarily concerned with military security and the latter with civil security. Despite the apparent differences of interest between the two units, their counterintelligence problems are interrelated. A dissident civilian population hampering the efforts of a civil affairs unit to establish effective administrative control in an area is also likely to be the primary source of support for guerrilla operations capable of disrupting logistics operations through sabotage, terrorism, and harassment attacks. The MAGTF headquarters

counterintelligence team is normally responsible for the counterintelligence support for these units. This includes support for installations and facilities dispersed through the combat service support areas. The number of team personnel supporting civil affairs units depends on the number of refugees to be identified in the area.

f. Counterintelligence Team Operations. Employment of the team and team operations in combat is influenced by the mission of the supported command. The mission assigned the team, and the tactical scheme of maneuver for the unit which the team is supporting, also influence the type of team control, methods of communication, equipment, deployment of subteams, and the determination of the team's area of operations and targets, including the development of a counterintelligence target-reduction plan. Based on the mission, the team commander formulates the plan for the employment of his team.

(1) Team Planning. The successful accomplishment of the team's mission requires thorough planning by the team commander. The following must be considered when planning for team operations:

- Detailed study of all available maps and photographs of the projected area of operations.
- Study of all available intelligence products pertinent to the area of operations.
- Location of all important targets and specific buildings on the map. These are categorized and studied and plans formulated for coverage and reduction. Target priorities must be assigned in advance to ensure efficient use of personnel. An estimate and follow-up request must be made for troop requirements and employment incidental to any *sealing off* or *uncovering* action. Marine Corps counterintelligence personnel are rarely available in sufficient numbers to handle such actions alone. The area surrounding a target is studied to determine points where *sealing off* would be most effective. Streets and approaches to targets are studied thoroughly, thereby minimizing the need for extensive physical reconnaissance. Main traffic routes are studied to determine locations in which to establish screening centers and checkpoints.
- Acquisition or development of black, gray, and white lists of persons in the target area. (See par. 503.)
- Study of all available records listing public officials opposed to the enemy and other persons who could be of value in administrative assignments, such as members of the police force, fire department, post office, railway, telephone, telegraph, and broadcasting stations. Much of this data can be obtained from civil affairs units and the various G-2/S-2 sections.
- Acquisition of available information concerning pro-American or antiopposition elements, such as guerrillas and partisans in the zone of operations and other areas, which would facilitate immediate utilization of such groups if necessary.
- Acquisition and study of all information concerning other underground forces, groups, and personnel who, by reason of training and experience, can provide assistance in the conduct of counterintelligence interrogations.
- Counterintelligence contingency materials (CICM), the Naval Intelligence Processing System (NIPS), and the Marine Air-Ground Intelligence System (MAGIS) segments, as well as other data bases, are valuable sources of information.

(2) Team Control. Control of the team operations is centralized under the team commander. Only in those situations where team operations require the detachment of subteams to subordinate commands and centralized control is unfeasible should operational control be released to the commanders of the units to which the subteams are attached.

(3) Tactical Deployment of the Team

(a) During both static and fluid tactical situations in populated areas, the team headquarters

normally is centrally located and easily accessible to indigenous personnel. Locating the team headquarters within a headquarters command post is undesirable since it must be accessible to indigenous personnel, thereby increasing the security problem. The team headquarters is located to provide maximum assistance to other agencies and to ensure protection by them if required; however, during fluid tactical situations in uninhabited areas, the team headquarters may be located in or near the supported unit's command post.

(b) In deploying team personnel, consideration is given to retaining at least one subteam at the team headquarters for special assignments and emergencies.

(c) When counterintelligence teams are held in reserve, team personnel are organized and equipped so that the augmentation subteams may be immediately dispatched when forward units require counterintelligence reinforcements.

(d) Subteams are attached to subordinate units sufficiently in advance to coordinate the former's plans and target reduction plan with the unit's scheme of maneuver and assigned mission.

(e) Whenever possible, subteams are employed in area rather than unit support. This permits the employment of as many personnel as required in areas where counterintelligence operations are extensive. Units whose zones of action do not require counterintelligence operations do not have counterintelligence personnel attached. The team commander must provide for the rapid detachment/attachment of subteams as the counterintelligence situation develops.

(f) In effecting the relief of a counterintelligence team, it is the responsibility of the team being relieved to turn over prisoners, records, and informants to the team assuming responsibility for the area. To make this transition as smoothly as possible, one or two men from the team relieved remain behind to familiarize the relieving team with the counterintelligence situation in the area, or representatives of the relief team are sent forward to effect familiarization with the counterintelligence situation.

307. Counterintelligence Operations

Counterintelligence operations in a combat environment require detailed planning and coordination. Counterintelligence operations are usually conducted in conjunction with, and require support from, other units. To be effective, all elements involved must be thoroughly briefed and knowledgeable of the purpose and objectives of the operation.

a. Counterintelligence Screening Operations. Counterintelligence screening operations are designed to identify and apprehend enemy intelligence agents, subversives, terrorists, and saboteurs attempting to infiltrate friendly lines or conceal themselves among the population. In a conventional warfare situation, screening operations primarily consist of screening refugees and prisoners of war and using checkpoints in populated areas.

(1) Coordination

(a) Refugee and prisoner-of-war screening is planned and coordinated, where possible, with military police elements, interrogator- translator teams (ITT's), civil affairs units, and pyschological operations elements.

(b) The tactical commander is primarily concerned with the movement of refugees and prisoners through his area without disrupting operations, and with obtaining information of tactical value from these refugees or prisoners. Screening operations must be compatible with the commander's scheme of maneuver.

(2) Preparation

(a) Prior to the operation, counterintelligence personnel must become thoroughly familiar with all available information concerning the enemy intelligence organization, the military and political situation within the enemy controlled area, and the geography of the area.

1. In order to successfully identify enemy intelligence agents, counterintelligence

personnel must be knowledgeable of the enemy intelligence organization, including its mission, methods of operation, officials, schools and training, known agents, and policies and regulations.

2 Knowledge of the political situation and of the restrictions placed on the population within the enemy controlled area aid in detecting discrepancies during the screening. Information required includes travel retrictions, curfews, draft and conscription regulations, civilian labor forces and work patterns, and the education system.

3 Obtaining order of battle information is primarily the responsibility of the interrogator-translator teams; however, counterintelligence personnel must be aware of the enemy military units operating within the area, and knowledgeable of their disposition, composition, activities, training, equipment, history, and commanders' personalities. This information aids in identifying military intelligence personnel or other persons attempting to hide their identity.

4 Counterintelligence personnel must also be familiar with the geography and the political, social, and economic conditions of the area. Travel conditions, distances, major landmarks, customs, and composition of the population are essential to the successful screening operation.

(b) Preparation for the operation also includes compiling a list of personnel of known counterintelligence interest, a list of indicators to aid in identifying persons of counterintelligence interest, and basic data sheets which may be completed on persons being screened. This information is distributed to key personnel participating in the operation to aid in identifying those persons requiring interrogation by counterintelligence personnel. The basic data sheets are filled out to aid in determining the individual's knowledge and in formulating questions for further interrogation. The basic data sheet contains, as a minimum, the following information:

- Basic identification data of the individual and his family including name, aliases, date and place of birth, sex, race, religion, citizenship, address, and marital status.
- Education and professional experiences.
- Knowledge of languages, foreign travel, military service, and technical qualifications.
- Political affiliations and membership in other groups and organizations.
- Details of current travel to friendly lines or point of capture, to include point of departure, times, and circumstances.
- Additional questions may be included which relate to specific indicators revealing areas of counterintelligence interest.

(3) Initial Screening

(a) Prisoners of war and refugees normally enter prisoner-of-war and refugee channels rearward of the forward edge of the battle area (FEBA) for further movement to rear areas. Initial screening is conducted as soon as possible after the prisoners of war or refugees come under friendly control. Initial screening is usually accomplished by unit intelligence personnel, ITT's, or counterintelligence personnel. In the case of a large number of refugees, assistance in initial screening may be provided by military police, civil affairs units, psychological operations personnel, and tactical troops, if available.

(b) Persons identified or suspected to be of counterintelligence interest are separated from other prisoners of war or refugees and referred to counterintelligence personnel for interrogation, after information of immediate tactical value has been obtained. Personnel of counterintelligence interest are exploited, if possible, and then evacuated to higher headquarters for further detailed interrogation and exploitation by rear area counterintelligence teams. Further counterintelligence screening also continues for

other prisoners of war and refugees at the higher echelons. Procedures for the handling of captured enemy personnel are contained in FMFM 2-1, *Intelligence*, and FM 19-40, *Enemy Prisoners of War, Civilian Internees, and Detained Persons*.

(4) Conduct of the Screening

(a) In many cases, numerous prisoners of war and refugees preclude counterintelligence interrogation of every individual. The initial screening is designed to identify those persons who are, or are most likely to be, of counterintelligence interest and who require interrogation by counterintelligence personnel. The success of the screening operation is, therefore, directly influenced by the degree of preparation and the quality of the information provided to personnel conducting the initial screening.

(b) Counterintelligence interrogation is designed to confirm or to deny that the person is of counterintelligence interest and to exploit the information obtained when appropriate. Persons who are determined not to be of counterintelligence interest are returned to the prisoner-of-war or refugee channels as appropriate. Those persons who are of counterintelligence interest are evacuated through counterintelligence channels for further interrogation and exploitation by rear area counterintelligence teams. An interrogation report is completed on each individual referred for further interrogation. This report clearly identifies those areas of counterintelligence interest and includes as much information as possible concerning the individual's identity and documentation, background, recent activities, and route of travel to friendly lines or point of capture. A sample format for the interrogation report is contained in appendix B.

(5) Indicators

(a) Indicators to aid in the identification of possible hostile infiltrators are determined after a thorough study of the enemy area, the political and military situation, and the enemy intelligence organization.

(b) For maximum effectiveness, indicators must relate to the specific area of operations; however, the following general indicators may serve as a guide to identify persons as possible infiltrators:

- Persons of military age who are not members of the armed forces.
- Persons without identification or with unusual or altered documents.
- Persons attempting to avoid detection or questioning, or displaying peculiar activity.
- Persons using enemy methods of operation.
- Persons possessing unusually large amounts of money, precious metals, or gems.
- Persons traveling alone or in pairs.
- Persons having a pro-enemy background, family members in enemy areas, or who have collaborated with the enemy.
- Persons with a suspicious story or who have violated regulations in enemy areas.

(6) Other Methods of Screening. In addition to interrogation, the following methods of screening can be used separately or in combination:

- Insertion of informants into prisoner-of-war and refugee channels and detention centers.
- Use of concealed informants at screening collection points.
- Use of sound equipment in holding areas.
- Polygraph examination.
- Specialized identification equipment.

(7) Mobile and Static Checkpoints

(a) Checkpoints are used in screening operations in populated areas and along routes of

travel to detect and prevent enemy infiltration of espionage, sabotage, terrorist, and subversive agents and to collect information which may not otherwise be available to intelligence units.

(b) The preparation for employment of mobile and static checkpoints is the same for other screening operations. Lists of persons known or suspected of enemy activity (black and gray lists), and of indicators, are normally utilized in the screening operation. Specialized detection equipment may also be used, if available.

(c) Checkpoints are established at strategic locations where sufficient space is available for conducting searches and assembling the people to be screened. Provision is made for the security of the checkpoint, and personnel are positioned to the front and rear of the checkpoint to apprehend those attempting to avoid it.

- A mobile checkpoint can be used as a moving system whereby the screening team, either mounted in vehicles or on foot, selects individuals to be stopped for questioning and a check of identity. The mobile checkpoint also may be established at various locations, usually for periods not to exceed 1 day.

- Static checkpoints are those manned permanently by military police or combat troops at entrances to towns, bridges, and other strategic locations.

(d) Screening teams may be composed of combat troops, intelligence interrogators, military police, counterintelligence personnel, civil affairs personnel, or a combination of such personnel. Screening teams conduct the initial screening and refer suspects to the counterintelligence element for interrogation and further exploitation.

b. Neutralization and Exploitation Operations

(1) Operational Support. The timely seizure and exploitation of counterintelligence targets require a detailed and coordinated plan that has been prepared well in advance. (Information on targets and target reduction can be found in paragraphs 503 and 504.) Counterintelligence teams, in most instances, cannot neutralize, guard, or physically control targets without assistance. In some cases, for the seizure and protection of well-defended targets, this assistance must come from ground combat units. In other cases, the assistance may be provided by combat support, combat service support, or aviation units. It is essential that the required assistance be provided for during the planning phase. Counterintelligence personnel will normally accompany the troops used in target reduction to advise, assist, and examine and/or exploit the target at the earliest possible time. In some instances, it may be advantageous for counterintelligence personnel to rendezvous with the assigned troops at the target area. Except in unusual cases, the tactical effort will take precedence over the neutralization and exploitation of counterintelligence targets. If assistance in target reduction is not available, counterintelligence elements may have to rely on their own assets to neutralize or exploit targets. In friendly controlled areas, counterintelligence elements may also receive assistance from civil police and security agencies.

(2) Target Personalities. Target personalities are often valuable sources of combat and strategic intelligence information. Information of immediate tactical value must be promptly obtained and the individual evacuated to higher headquarters as soon as possible. If evacuation is to be delayed due to the tactical situation, a report of the circumstances must be forwarded to higher headquarters so that arrangements may be made for further interrogation, exploitation, and disposition when the tactical situation permits. It is essential that target personalities be handled separately and that they remain out of contact/association with prisoners or other persons detained or being evacuated.

(3) Target Installations. The exploitation of installations should be accomplished by counterintelligence personnel immediately following the neutralization of the installation if the tactical

situation permits. The installation is searched thoroughly for documents, equipment, and other material of intelligence or counterintelligence interest. Procedures for the disposition of enemy documents and material are contained in FMFM 2-1, *Intelligence*. In some instances, it may be desirable to retain the documents or material within the installation for thorough examination by technical intelligence personnel or other specialists. Due to explosive devices (i.e., boobytraps, mines, etc.), extreme caution should be used when searching installations known or suspected to have been occupied by the enemy.

c. Investigations and Internal Security Functions

(1) Investigations. During combat operations, counterintelligence personnel may be required to conduct investigations concerning personnel, security matters, espionage, sabotage, terrorism, and subversive activities (including defection). The investigation is a duly authorized, systematic, detailed examination/inquiry to uncover and report the facts of a matter. While facts, hearsay, information, opinions, allegations, and investigators' comments may make a significant contribution, they should be clearly labeled as such in the report of investigation. The Naval Investigative Service manual, NIS-3, *Manual for Investigations,* may be used as a guide for investigation techniques and procedures.

(a) Counterintelligence investigations utilize basic investigative techniques and procedures and are designed to detect, prevent, and/or neutralize actual or potential threats to the security of the command. The primary purpose of the investigation is to provide the commander with sufficient factual information to reach a decision or to ensure the security of his command.

(b) Investigations may be conducted overtly or discreetly depending on the type of investigation and the area of operations. Investigations will normally include the examination of records, interviews or interrogations, and the collection and handling of evidence. Surveillance and the conduct of raids and searches may also be appropriate as the investigation progresses.

(c) Upon assumption of primary counterintelligence jurisdiction, counterintelligence investigations will be conducted in accordance with guidance contained in NIS-3, *Manual for Investigations,* and instructions published by the MAGTF commander.

(d) Certain unique problems are involved in conducting investigations of indigenous personnel in a tactical environment. Counterintelligence personnel are normally responsible for conducting security investigations of indigenous personnel employed by FMF units and may also be involved in the investigation of indigenous personnel retained in official civilian positions. Difficulty in investigations often will be encountered due to a lack of files and records in the repositories of civilian police and investigative agencies, as such documentation may have been destroyed or removed during tactical operations. Every effort must be made to check all files and records which are available. Special investigative techniques, such as the use of polygraph examinations by criminal investigative personnel, may be required. The utilization of indigenous personnel by FMF units presents a definite security threat because of the enemy's efforts to penetrate units through the use of indigenous civilian employees who are sympathetic to, or may be coerced into serving, the enemy cause. All units utilizing indigenous personnel must exercise caution to preclude the enemy's collection of information, both classified and unclassified, useful to the him. In addition to the initial security investigation, continual checks are made on employees. Counterintelligence elements maintain close liaison with the civil affairs units responsible for providing civilian labor to military forces.

(2) Troop Movement Security. The movement of troops is of vital concern to the enemy and, in many cases, may provide the first indication of friendly intentions. Enemy intelligence activity

may be expected to increase prior to, during, and immediately after the movement of troops. Troop movement security is designed to deny the enemy as much information as possible, to prevent espionage and sabotage from interfering with the movement, and to ensure the element of surprise. Counterintelligence personnel coordinate closely with the commander's staff and provide security services and assistance as required.

(a) Some of the services and assistance normally provided by counterintelligence personnel include the following:

- Providing advice and assistance on security matters during the preparation of plans for the movement.
- Conducting counterintelligence evaluations and inspections, providing recommendations for maximum secrecy, and assisting in instructions to unit personnel concerning troop movement security.
- Observing the move, investigating and reporting security violations, and providing briefs on other security threats.

(b) The following security measures must be considered regardless of the type of transportation utilized for the move:

- Imposing the Wartime Information Security Program.
- Monitoring or restricting communication facilities.
- Increasing emphasis on security education programs.
- Gradually reducing leave and liberty, if appropriate.
- Surveillance of areas and facilities where loose talk may be prevalent.
- Removing or covering tactical markings and other identifying marks on vehicles and equipment.
- Providing instructions for the storage or destruction of personal diaries, mail, and other documents and papers.
- Arranging for special issue of equipment and clothing, and for other administrative activities in such a manner that will minimize the indication that a move is imminent.
- Covering and guarding certain material and equipment to conceal its identity and preclude unauthorized access during the move.
- Providing security guards at loading points, at critical areas along the route, and at the destination.
- Inspecting vacated areas to ensure that nothing of intelligence value has been left which might indicate the destination, identity, or mission of the unit.
- Inspecting and evaluating the destination area for physical security hazards when possible.
- Deceptive actions designed to mislead the enemy when approved by the senior area commander or higher authority.

(3) Counterintelligence Surveys, Evaluations, and Inspections. In a combat environment, counterintelligence surveys, evaluations, and inspections, including TSCM inspections and surveys, are conducted in essentially the same manner as during garrison operations (see sec. 4); however, counterintelligence surveys and TSCM inspections and surveys are usually limited to permanent installations in rear areas. In those instances where perimeter security is the responsibility of a tactical unit, the physical security portion of the counterintelligence survey is primarily concerned with those areas within the perimeter containing classified material and areas susceptible to sabotage and terrorist attack. Special weapons sites require extra emphasis and may include counterintelligence monitoring of shipments in addition to other security services.

(4) **Port and Harbor Security.** Port and harbor security is normally provided jointly between military police and the counterintelligence elements supporting the logistics command operating the port. Counterintelligence elements concentrate their efforts on counterintelligence security procedures and special operations.

- Counterintelligence security procedures for ports and harbors are essentially the same as those required for installations, with the addition of controls established for ships and their crews. Special emphasis is required for ships under a foreign flag.

- Special operations place emphasis on hostile sabotage and subversive activity. Special operations are normally required within the port as well as the surrounding area.

d. Special Operations. Special operations are conducted by counterintelligence personnel and require detailed planning, coordination, and control. (See par. 303e.) Procedures for the conduct of special operations are contained in FM 30-17A, (C) *Counterintelligence Special Operations* (U).

e. Intelligence Collection

(1) Counterintelligence teams can collect both counterintelligence and combat intelligence information through the use of HUMINT resources. In addition to its counterintelligence functions, a team may be assigned additional responsibility for combat intelligence collection, particularly in low counterintelligence threat areas; however, care must be exercised to ensure that these responsibilities do not impair the accomplishment of the overall counterintelligence mission.

(2) The procedures and authority for the conduct of human intelligence operations and certain special operations are normally provided by the senior area commander. Guidance and operational procedures for HUMINT operations are contained in DIAM 58-11, Volumes 1 and 2, and FM 30-18, (S) *Intelligence Collections Operations* (U).

f. Wartime Information Security Program

(1) The WISP is designed to control and examine communications to prevent disclosure of information of value to the enemy and to collect information of value to the United States.

(2) DOD Directive 5230.7 assigns responsibility and provides guidelines for WISP planning within the Department of Defense, to include national, armed forces, civil, enemy prisoner of war and civilian internee, and field press WISP's.

(3) OPNAVINST 5530.6B is a Joint Service directive which provides basic policy and guidance for commanders in the establishment and operation of the U.S. Armed Forces WISP. Armed Forces WISP is the examination and control of personal communications to or from persons in the Armed Forces of the United States and persons accompanying or serving with the Armed Forces of the United States.

(4) OPNAVINST 5530.0A is a Joint Service directive which provides basic policy and guidance for commanders in the establishment and operation of civil WISP, the review of civilian communications, such as messages, printed matter, and films, entering, leaving, or circulating within areas or territories occupied or controlled by the Armed Forces of the United States.

(5) OPNAVINST 5530.11 is a Joint Service directive which provides basic policy and guidance for the establishment and operation of WISP for the incoming and outgoing communications of enemy prisoners of war and civilian internees held by the United States military authorities outside the limits of the United States and Puerto Rico.

(6) Additional responsibilities are published by unified and specified commanders, type commanders, fleet and numerical fleet commanders, special commanders, and area coordinators.

(7) Fleet Marine Force units are primarily concerned with Armed Forces WISP, the objectives of which are to prevent the disclosure of information that might assist the enemy or adversely affect any policy of the United States, and to collect and disseminate information to assist the United States in the successful prosecution of a war.

(8) Fleet Marine Force units must be prepared to institute WISP when directed; WISP is a functional responsibility of the G-1.

308. Tactical Counterintelligence Interrogation

Within the area of operations, there may be numereous people who are viewed as threats to security, perhaps solely due to their presence in the combat zone. The number of suspect personnel will vary, but frequently it will preclude detailed interrogation of all but a selected few who are of primary interest. Counterintelligence personnel will be partly dependent upon such agencies as the provost marshal, civil affairs units, and interrogator-translator units (ITU's) to identify suspect persons or persons of counterintelligence interest. In some situations, the number of persons volunteering information to counterintelligence operation permits concentration on those of the greatest potential interest or value. Most suspects are apprehended while trying to enter the area, or their cover stories (which will closely parallel their true places of origin and identities) are exposed. The counterintelligence interrogator's success in such interrogations is primarily dependent upon his questioning skill, linguistic ability or support, knowledge of the area of operations and adjacent areas, and familiarity with the intellectual, cultural, and psychological peculiarities of the persons encountered.

a. Types of Subjects. As the battlelines in combat change, entire segments of the population may be overrun. The local population in any area may also be increased by refugees and displaced persons (persons from other countries conscripted by enemy forces for labor). The following categories of persons are of counterintelligence interest:

- Refugees and displaced persons.
- Line crossers.
- Deserters from enemy units.
- Civil prisoners.
- Enemy intelligence personnel.
- Inmates of enemy detention camps.
- Members of underground resistance organizations seeking to join friendly forces.
- Collaborators with the enemy.
- Target personalities, such as black, gray, or white list personalities.
- Volunteer informants.
- Persons who must be questioned because they are under consideration for employment with FMF units or for appointment as civil officials.

b. Objectives of Counterintelligence Interrogations. The counterintelligence interrogation in combat areas assists in the accomplishment of three major objectives:

(1) In the screening process, refugees whose very presence threatens overall security are removed from the battlefield.

(2) In detailed interrogations, enemy agents with espionage, sabotage, terrorist, or subversive missions are detected.

(3) The wide range of activities permits the collection of information of value to other intelligence and security agencies and to the planners of military operations. Counterintelligence interrogators must be especially alert to obtain and report information of immediate tactical value which may not have been previously obtained or reported.

c. Indicators Warranting Suspicion. Counterintelligence personnel must be alert during interrogations for indications of intelligence activity. Indicators which, separately or collectively, may generate suspicion that a subject is in the employ of, or acting in sympathy with, enemy forces are as follows:

(1) Access to Information or Targets. A prospective terrorist, subversive, espionage, or sabotage agent must have access to the information desired by the enemy or to the target installation to be destroyed in order to carry out his mission. The interrogation should establish a subject's accessibility to potential targets, including his location at the time he was apprehended.

(2) Technical Skills. Proficiency in certain technical skills is frequently an attribute of an espionage or sabotage agent. The subject who has a mastery of one or several foreign languages and a knowledge of radio operation or cryptography is questioned carefully on the nature and purpose of his training in those fields. His practical experience and his work in those fields, during or shortly prior to the war, should give counterintelligence personnel cause for strong suspicion, and the individual's story must be closely examined.

(3) Documents and Funds. An overabundance of documents and new documents of questionable authenticity are reason for doubt and provide the basis for detailed questioning. Discrepancies in the document's contents or conflicts between data and the subject's story may lead to the detection of hostile agents. Unexplainable possession of large amounts of money, valuable jewelry, or other items of great value are investigated carefully.

(4) Pro-Enemy Background. Residence or travel in enemy territory, membership in a hostile party, or known former collaboration with the enemy are facts of obvious importance. Counterintelligence personnel must determine whether the subject is actually in sympathy with the enemy or has acted merely to serve his own best interests with regard to his life, the welfare of his family, or his property.

(5) Family in Enemy-Held Territory. Enemy pressure is often applied to individuals whose families reside under enemy control, particularly if the family has no past connection with the enemy-held area.

(6) Inconsistent Story. Small discrepancies in the subject's story may be important. Distance compared to travel time; accent peculiar to an area the subject refuses to acknowledge as his own; unreasonable explanation of deferment, exemption, or discharge from military service; exemption from labor conscription; or implausible reasons for risking the crossing of combat lines may be warning signals to the counterintelligence interrogator. Contradictions in a subject's story do not warrant jumping to conclusions; however, counterintelligence personnel must remain alert to all possibilities. Allowances must be made for defective memory or lack of logic due to emotional stress.

(7) Suspicious Actions or Activities. Unusual interest displayed by indigenous persons in troop units or equipment, or persistent loitering in the vicinity of troop units and installations without reasonable explanation, are sufficient to warrant interrogation for the purpose of clarifying the status of a person so involved.

(8) Violations of Civil or Military Regulations. Mere violation of military regulations in an area controlled by the military, such as mandatory registration, curfews, travel restrictions, or declaration of weapons, may be relatively unimportant to counterintelligence elements. However, the motives which cause such violations despite severe penalties must be compelling and possibly may be of great interest to counterintelligence personnel.

(9) Modus Operandi. The frequent similarity in tactics of hostile agents working for the same enemy agency, their means of contact with their agent handlers, type of cover story, and manner of collecting and reporting their information may lead to identification of suspects with a known enemy agency or group. Established patterns of

activity or behavior of enemy agents are disseminated to other intelligence and security agencies to assist in the identification of agents still operating.

d. Screening or Initial Interrogation. Initial interrogation and screening are generally synonymous, except that the former indicates that there will be a follow-up detailed interrogation, while screening involves the selection, by brief questioning, of a relatively small number of persons from a large group, for detailed interrogation. In both cases, the technique, purpose, and scope of the questioning are generally the same. The object is to select for detailed interrogation, a reasonable number of persons who appear to be suspect or knowledgeable on matters of counterintelligence interest. Initial interrogation or screening is generally concerned with identity, background, recent activities, travel or escape routes, and information of immediate value. Documents and personal belongings of a subject are examined; the circumstances of apprehension are studied; and available files are checked.

e. Detailed Interrogation. Detailed counterintelligence interrogations may be conducted in joint interrogation centers or at interrogation sites established by intelligence or counterintelligence units. Detailed interrogation does not differ radically from the initial interrogation except that attention is now focused on individuals who are suspect or who are known to have extensive information of interest. A study of the initial interrogation report, examination of the subject's documents and belongings, and checks of avilable files and information must be conducted and analyses made in preparation for the interrogation.

(1) Details of the subject's personal history must be reviewed. Should the subject admit that he is an enemy agent, he becomes an important source of information on enemy intelligence methods of operation and, perhaps, on identities of other hostile agents. This will lead to exhaustive interrogations on such issues as hostile intelligence, training, and missions assigned. However, counterintelligence personnel must be alert to the possible insertion of confusion agents.

(2) The suspect, or any person being interrogated, may also be an important source of information of intelligence value, strategic and/or tactical.

(3) The questioning usually follows a logical sequence to avoid confusing the subject and to facilitate reporting; however, an illogical sequence may be used as a technique to purposely confuse the subject so that he will inadvertently contradict himself. The interrogator must be alert for discrepancies and retain his psychological advantage.

(4) Specific techniques of interrogation are discussed in FM 30-15, *Intelligence Interrogation*.

f. Operation of a Counterintelligence Interrogation Center

(1) A counterintelligence interrogation center serves as a centralized location where persons of counterintelligence interest are interrogated. In offensive situations where assault unit counterintelligence teams are reducing priority counterintelligence targets, it may be necessary for higher echelons to assume the interrogation responsibility at the lower echelon. For this, the use of augmentation subteams is of value. Each major command with counterintelligence support normally establishes such interogation centers, thereby supporting the concept of counterintelligence coverage in depth.

(2) A centrally located counterintelligence interrogation center is placed in operation as soon as possible. In a static situation when the counterintelligence team has no immediate offensive targets, consideration may be given to selection of a building that will provide adequate facilities, such as a waiting room for arrivals, an interrogation room, a detention room, and a waiting room for departures. In fast-moving situations, interrogation centers are necessarily moved rapidly and frequently. All units concerned with disposition of line crossers, refugees, etc., must be kept notified as to the location of interrogation centers. Additionally,

arrangements must be made for the guarding and disposition of line crossers, refugees, and other persons processed at such installations.

(3) The counterintelligence interrogation center is normally established in the vicinity of the prisoner-of-war compound/collecting point, or in a secure location specified by the operational counterintelligence team/subteam commander. Regardless of location, a close working relationship is established between counterintelligence and interrogator-translator units. Routine prisoner-of- war interrogation is not a function properly assigned to the counterintelligence team. Team personnel are utilized to interrogate only those prisoners who have been determined to be of counterintelligence interest.

(4) All persons detained are handled and treated in accordance with the applicable Geneva Conventions. (See FM 27-10, *The Law of Land Warfare*.)

309. Friendly Prisoners of War and Persons Missing (Nonhostile) and Missing in Action

Friendly personnel who fall into the hands of the enemy can be a source of information through the compromise of documents, personal papers, or as the result of effective interrogation or coercion. It is incumbent upon the tactical commander to counter this threat by taking those steps necessary to counter any possible disclosure which would affect the immediate tactical situation. Counterintelligence units are assigned responsibility for the collection of information of potential intelligence value on friendly personnel possibly in enemy hands and the collection of intelligence information to aid in identifying, locating, and recovering those personnel. In addition, counterintelligence personnel conduct the intelligence and counterintelligence debriefings of those Marines who have been detained by the enemy and returned to friendly control, as well as those personnel who were recovered or who evaded capture during an incident resulting in the capture or missing status of a Marine, hospital corpsman, or other assigned personnel.

Marine Corps commands notify the nearest counterintelligence unit when Marine Corps personnel, including hospital corpsmen or other assigned personnel, are captured or determined to be missing (nonhostile) or missing in action. The counterintelligence unit may be able to provide information which could aid in the search and recovery efforts, such as possible routes to enemy detection centers, location of possible holding areas, and enemy procedures for handling and evacuating prisoners. If appropriate, the counterintelligence element can also initiate immediate collection action utilizing counterintelligence sources to gain information for possible recovery or search and rescue operations.

If the search or recovery attempts are unsuccessful, the counterintelligence unit initiates an immediate investigation to gather basic identification data and to determine the circumstances surrounding the incident. The investigation is designed to provide information to aid in subsequently identifying and locating the individual, to assess the potential intelligence gain if the individual is held, and to collect intelligence information which will be of value when evaluating future intelligence reports. Format for the basic identifying data required is contained in appendix A. Every attempt is made to obtain a recent photograph and a sample of the individual's handwriting. A synopsis of the investigation, including a summary of the circumstances, is prepared on the counterintelligence report form (NAVMC 10481 [Rev ___]). The completed basic identifying data form is attached as an enclosure to this report. The investigation must be as thorough and detailed as possible and classified according to content. In the case of aircraft incidents, the investigation includes type of aircraft, location and sensitivity of classified equipment, bureau or registration number, call signs, and any aircraft distinguishing marks, such as insignia, etc. When feasible, the investigator should coordinate with the accident investigation team or aviation safety officer of the unit which experienced the loss.

The counterintelligence report with the attached personnel data form is distributed to the following commands:

- * Commandant of the Marine Corps (Code INT).
- * Appropriate headquarters (Fleet Marine Force Pacific [FMFPAC] or Fleet Marine Force Atlantic [FMFLANT]).

- * Marine air-ground task force headquarters.
- Individual's parent command (division, wing, or MAB).
- Each counterintelligence team in the combat area.

These reports are designed to aid in the counterintelligence mission and are not intended to replace the normal casualty reporting procedures. When the counterintelligence report concerns a member of another Service assigned to a Marine Corps unit, a copy of the report is also provided to the appropriate Service organization. All subsequent information, which pertains or may pertain to persons captured or missing in action, is distributed in the same manner as the initial counterintelligence report.

Marine Corps personnel returned to friendly control after being detained by the enemy are debriefed by Marine Corps counterintelligence personnel. Normally, counterintelligence personnel supporting the unit which first gains custody of the individual conduct an initial debriefing for information of immediate tactical value and the location of other prisoners of war in the area. As soon as possible, the returnee is evacuated to the MAGTF headquarters for further debriefing or for evacuation to a debriefing site as determined by higher headquarters. Upon return of a person who was captured, listed as missing (nonhostile), or missing in action, those commands listed (*) in paragraph 309 are immediately notified. Specific guidance for the processing and handling of Marine Corps personnel captured or missing in action is contained in applicable Marine Corps orders.

310. Counterinsurgency Operations

To effectively conduct counterintelligence operations in an insurgency environment, counterintelligence personnel must be thoroughly familiar with the nature of insurgency—its causes, characteristics, and peculiarities. Information concerning counterinsurgency operations and intelligence and counterintelligence applications are contained in FMFM 8-2, *Counterintelligence Operations*; FM 30-17, *Counterintelligence Operations*; and FM 30-17A, (C) *Counterintelligence Special Operations* (U).

Insurgency efforts are directed and highly controlled by a *hard core* insurgent infrastructure which employs an extensive intelligence network. Basic responsibilities of counterintelligence units in an insurgency environment are the denial of information to the insurgent force and the identification and neutralization of the insurgent infrastructure, with emphasis placed on its intelligence apparatus.

Counterinsurgency operations basically are aimed at the restoration of internal security in the area of operations, which requires a vigorous and highly coordinated counterintelligence effort. The nature of insurgency and its covert methods of operation require the employment of a greater number of counterintelligence personnel than is necessary for conventional operations.

a. Jurisdiction. The commitment of Marine Corps forces for counterinsurgency operations is normally covered by a status of forces agreement which may include limitations and restrictions concerning the investigation and apprehension of host country citizens or other operations matters. Host country counterintelligence, security, and law enforcement agencies usually are extensively engaged in counterintelligence and security operations prior to the arrival of U.S. forces. Counterintelligence units may be assigned to assist these agencies; however, Marine Corps counterintelligence teams are normally employed in support of Marine Corps units. Effective counterintelligence operations require extensive coordination with host country intelligence, counterintelligence, security, and law enforcement agencies.

b. Employment of Counterintelligence Teams

(1) The employment of counterintelligence teams in counterinsurgency operations is similar to that described in paragraph 306. Area coverage is usually preferred to provide continuity of operations and to ensure continuous coverage of the area. The insurgent infrastructure and intelligence apparatus usually have been operating within a given area for many years and are thoroughly familiar with all aspects of the area and its people.

Continuity of operations and other characteristics of the area coverage concept are particularly suited to counter the insurgent intelligence threat.

(2) In assigning any areas of responsibility, ensure coverage overlaps to preclude gaps occuring between areas. Insurgent forces usually prefer to operate on the political or military boundaries where the assigned responsibilities of U.S. and allied forces may be vague and coordination is more difficult. Counterintelligence teams employed through unit assignment also are assigned responsibility for the area of influence around the unit's tactical area of responsibility (TAOR). Under the unit assignment concept, rear area counterintelligence teams assume responsibility for any gap in coverage that may develop.

c. Counterintelligence Measures and Operations

(1) The basic counterintelligence operations, techniques, and procedures previously discussed in this section are generally applicable in an insurgency environment. Both passive and active counterintelligence measures must be increased and aggressively pursued to effectively thwart the insurgent strategy.

(2) All commands must institute and continuously enforce counterintelligence and security measures to deny information to the insurgent force and to protect the command from sabotage. In coordination with host country authorities, emphasis is placed on security measures and checks of indigenous employees or other persons with access to installations or commands.

(3) A significant factor in counterinsurgency operations is population and resources control. The movement channels and patterns necessary for support, communications, and operations of insurgent forces are observed and controlled. Prior to implementing control measures, the population should be informed of the reasons for controls, and whenever possible, such controls should be performed and enforced by host country agencies.

(4) Counterintelligence teams must implement imaginative and highly aggressive special operations and HUMINT collection programs targeted against the insurgent infrastructure and guerrilla forces. The primary objective of special operations is the identification, location, and neutralization of specific members of the insurgent infrastructure through systematic intelligence collection and analysis with complete documentation concerning the activities of each individual. This allows the host country to be provided with an account of the individual's illegal activities once the person is apprehended. Penetration of the infrastructure must be obtained at all levels possible. Human intelligence operations are implemented to cover critical areas to identify and locate insurgent forces. Information derived from HUMINT programs may also be useful in special operations.

(5) In counterinsurgency operations, cordon and search operations may be employed to ferret out the insurgent infrastructure as well as individual unit elements which may use a community or area as cover for their activities or as a support base. The cordon and search operation basically consists of security forces which surround the area, usually at night, to prevent persons from leaving the area; a sweep element which escorts the people to a collection point at first light; search elements which search the area; and screening elements to process and screen the people for identification of known or suspected infrastructure or guerrilla force personnel. Cordon and search operations should be conducted in conjunction with host country forces and organizations, with U.S. forces, including counterintelligence units, providing support, advice, and assistance for the entire operation. As a minimum, host country personnel should be part of the screening and sweep elements of any cordon and search operation. The operation is often conducted in conjunction with medical, civil affairs, and psychological operations programs which are accomplished after the screening phase. Throughout the operation, care must be exercised to prevent an adverse psychological effect on the populace. Details concerning

the intelligence and counterintelligence aspects of cordon and search operations are contained in FM 30-17, *Counterintelligence Operations.*

311. Counterintelligence Funds

Special funds for conducting counterintelligence operations and intelligence collection activities by counterintelligence teams are available at higher headquarters. These funds may be made available upon request from the MAGTF. Procedures for the use, control, and accountability of funds are provided by the issuing headquarters.

312. Files and Reports

a. Files. Counterintelligence teams are responsible for establishing and maintaining operational files essential to their combat counterintelligence mission. The following operational files are normally maintained in a combat environment:

- Information concerning personalities, organizations, and installations of current and future counterintelligence interest. Often basic information of this type also is recorded in a card file or automatic data system (ADS) for ready reference and is cross-indexed to more detailed information.
- Correspondence and reports concerning specific operations and investigations.
- Source records containing essential data on sources of information.
- Area files containing basic reference data and information on enemy intelligence activity and counterintelligence measures within a particular geographic area.

b. Reports. The accomplishment of the counterintelligence mission requires accurate, timely, and pertinent reports disseminated in a usable form. Counterintelligence reports are prepared to transmit accurate information to units that can take action, to aid in the processing of intelligence, and to serve as a record of counterintelligence activities. The method of dissemination of counterintelligence information depends primarily on the nature and urgency of the information, the location of the receiving units, the security requirements, and the means available. Normally, information is disseminated by message, personal liaison, radio, telephone, briefings, messenger, and written reports. Sample formats for preparation of counterintelligence reports are provided in appendix B and may be modified for electrical transmission. Reports are classified according to content.

(1) Spot Report. Spot reports are used to rapidly report and disseminate information of immediate value. These reports are not limited to any specific type of information but must contain sufficient detail to answer basic interrogatives (who, what, when, where, why, and how). A requirement for speed in reporting and disseminating establishes the criteria for use of the spot report. Information contained in a spot report later included in another report must be clearly identified as having been previously reported so as not to be considered as confirming information. Source and information evaluation will be included on all spot reports together with the coded source identification, when applicable.

(2) Counterintelligence Information Report. The information report is the basic form for reporting collected counterintelligence/intelligence information. Information is normally reported by subject category and includes an initial evaluation of the source and the information. Significant information addressing national requirements will be reported by the MAGTF staff counterintelligence officer (SCIO), utilizing DD Form 1396. The counterintelligence information report format has been revised to coincide with DD Form 1396 format. (See DIAM 58-2A, Vol 2 for further guidance in completing DD Form 1396.)

(3) Counterintelligence Interrogation Report. The interrogation report notes the results of interrogations of counterintelligence interest. Designed to

provide information essentially of counterintelligence interest, it also contains information which could aid other intelligence organizations/agencies in their evaluation of any possible interest in the persons interrogated. Often, higher headquarters will require that certain information/reports initially be submitted on all persons captured or detained. In cases where a person is of interest to both counterintelligence and intelligence interrogators, close coordination with ITU's is required to ensure the proper submission of reports.

(4) Counterintelligence Report Form. The counterintelligence report form 3850 (NAVMC 10481 [Rev ____]) will be used to report the results of counterintelligence investigations, surveys, evaluations, and inspections. When longer than two pages, the first page of the report contains a synopsis. For uniformity and ease of report writing, the counterintelligence report normally contains five major sections—predication, purpose, background, results, and comments or recommendations. Enclosures to the report are designated in numerical order and are used to amplify or confirm information contained in the report. In the case of physical security evaluations for the storage of classified material, a locally produced security evaluation checklist may be used as an enclosure to the standard report form in lieu of lengthy written comments.

(5) Counterintelligence After-Action Report. After-action reports are prepared by counterintelligence teams to report the results of counterintelligence operations or operations which were supported by counterintelligence personnel and involved significant counterintelligence aspects. In addition, these reports serve as a record of tactical counterintelligence support activities within an area.

313. Communications

a. Capabilities. Each counterintelligence team possesses organic radio equipment to enable coordination of activities and the reporting of information to the level upon which it can be acted. Internal and external wire communications are established by the supported command as required.

b. Communication Requirements

(1) A counterintelligence tactical net should be established for each counterintelligence team. In addition, consideration should be given early in the planning to the establishment of a station on the counterintelligence tactical net. Coordination should be established with the communications-electronics officer to obtain radio element augmentation to support this station.

(2) Internal and external wire communications also must be planned for and coordination effected with the communications-electronics officer.

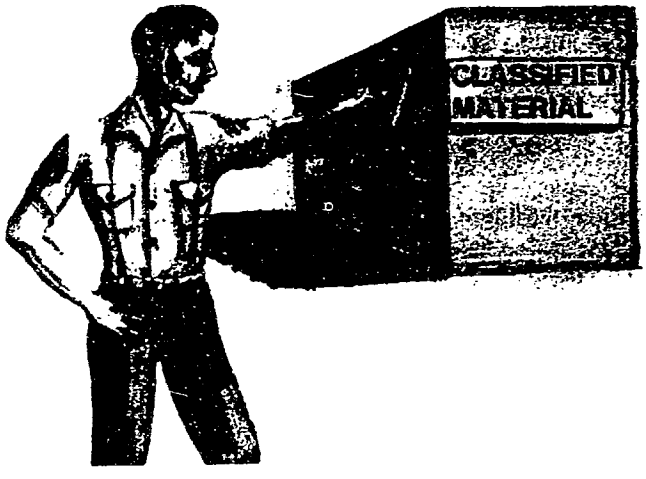
(3) Where feasible, counterintelligence circuits should be secure to preclude compromise of sensitive information.

c. Communication Management

(1) Staff counterintelligence officers/team commanders must coordinate with the communications-electronics officer regarding frequency allocation and assignment. Also, particular attention must be given to allocating available resources for the establishment of a station for the staff counterintelligence element on the counterintelligence tactical net.

(2) Consideration should be given to planning the use of various frequencies for agent communications.

(3) FMFM 10-1, *Communications*, provides additional information regarding communication systems, concepts of operation, planning, training, maintenance, and communications security for the Fleet Marine Forces.



Section 4

Counterintelligence Garrison Operations

401. General

The primary peacetime/garrison mission of counterintelligence teams is planning, preparing and training to accomplish their combat counterintelligence and human intelligence (HUMINT) functions. Secondarily, counterintelligence teams provide certain counterintelligence services to enhance the security of the command against espionage, sabotage, terrorism, subversion, and inadvertent disclosure or compromise of classified material.

Guidance for the planning and conduct of combat counterintelligence operations and for training are provided in sections 3, 5, and 6. This section provides guidance for conducting Marine Corps counterintelligence services while in garrison.

402. Counterintelligence Survey

The counterintelligence survey is designed to assist commanders in establishing systems, procedures, and safe guards to protect military installations, personnel, and organizations from espionage, sabotage, terrorism, and subversion. To determine the requirements for security, the survey includes an analysis of counterintelligence factors influencing security at the installation, a determination of the counterintelligence measures required by the sensitivity or criticality of the installation, an assessment of the counterintelligence measures which currently exist, and recommendations to bring existing counterintelligence measures to the required standard.

The counterintelligence survey is not a recurring service. The purpose of the survey is to establish requirements to

fit a specific installation, rather than to test compliance with requirements already established. Once a counterintelligence survey has been conducted, it remains valid unless there are major changes in the physical security characteristics of the installation, the mission of the command, or the potential threat.

a. Initiation of a Counterintelligence Survey. The request for a counterintelligence survey originates with the commander of the installation concerned or with a higher commander in the same chain of command. Counterintelligence surveys are normally requested for the following reasons:

- Activation or reactivation of an installation or major command.
- Significant change in mission or functions, or a major physical reorganization of an installation or major command.
- New, hazardous conditions within an installation which necessitate the reevaluation of the security system.
- Significant changes in classified material produced, processed, stored, or handled.
- Change in locale or environment in which the installation is located.
- Upon determination that a record of a previous survey does not exist.
- Upon a major change in potential threat to the installation.

b. Preparation for Counterintelligence Surveys

(1) Selection of Personnel. The number of personnel used to conduct the survey will vary depending on the size and nature of the installation, the availability of counterintelligence personnel, and any special operational or technical considerations. If possible, the survey team should include personnel who have been trained in methods of entry, computer system security, technical surveillance countermeasures (TSCM), and photography.

(2) Collection of Data. Prior to conducting the survey, the survey team must become as thoroughly familiar with the installation or command as possible. Information concerning the mission, organization, functions, security directives, and previous surveys, evaluations, and inspections of the installation/command provides valuable back ground and reference data. The files of intelligence and investigative organizations as well as those of the provost marshal's office may provide information on particular security hazards or problems. A complete set of security regulations is compiled for ready reference during the survey. Security regulations for reference during a counterintelligence survey include but are not limited to the following:

- DODINST 5200.1R (to be used as a reference when reports are forwarded outside the Department of the Navy.
- SECNAVINST 5521.6____.
- OPNAVINST 5510.1____.
- OPNAVINST 5510.45____.
- Applicable Marine Corps orders in the 5500 series.

(3) Coordination. Prior to initiating the survey, a counterintelligence representative contacts the commander of the installation/organization to be surveyed (or his representative) to coordinate the following matters:

- Determination and coordination of the proposed scope of the survey.
- Arrangements for access to necessary records, buildings, offices, and other areas.
- Procurement of applicable security directives, if not previously acquired.
- Arrangements for a survey team escort, if required.

- Arrangements for an initial briefing of key personnel on the purpose and objectives of the survey, if desired.

(4) Preparation of Checklists. The study and analysis of data collected on the installation or organization to be surveyed may indicate the necessity or desirability of preparing checklists to serve as a guide for personnel conducting the survey. The checklist notes general or specific points to be covered and serves as a reminder to surveying personnel to satisfy the predetermined scope of the survey. General points to be covered are common to all installations and organizations and include document, personnel, and physical security. Each of these major divisions are comprised of many subdivisions.

(a) Document security considerations may include storage containers, marking and handling of classified documents, application of *need-to-know*, duties of security control personnel, downgrading procedures, maintenance of classified document logs and receipts, and destruction procedures.

(b) Personnel security includes all aspects of the security clearance procedures, including clearance termination and the security education program.

(c) Physical security includes perimeter fencing, lighting, guard system, visitor control and pass systems, restricted areas, and building security.

c. Conduct of Counterintelligence Survey

(1) Preliminary Exterior and Interior Checks. The survey begins with a tour of the installation and the surrounding area to familiarize the survey team with the physical layout of the former and its relationship to the latter. During this tour, the survey team locates those areas, buildings, or offices which require special security considerations or which are considered to be sensitive. After the tour, it may also be necessary to interview certain staff officers to determine the operational importance of particular areas or buildings.

(2) Determination of the Installation's Sensitivity. Analysis of the collected data, and the tour of the installation and surrounding area, permit the survey team to make a preliminary evaluation of the installation's importance to national defense and its vulnerability and value as an espionage, terrorist, or sabotage target. An accurate appraisal of the security needs of the installation in relation to its sensitivity and importance is next required so that specific recommendations are commensurate with actual security needs. In determining the installation's sensitivity, the following are considered:

(a) **Mission.** The first consideration is the mission of the organization being surveyed. It must be determined if the mission is continuous or of short duration, unclassified or classified, and if technical or highly skilled personnel are necessary for its successful operation.

(b) **Cost of Replacement.** In estimating the cost of replacement of the installation, a comparative analysis (not a dollar and cents figure) is made. The time necessary to replace personnel, documents, and materiel in the event the installation is neutralized or destroyed is estimated. Further consideration is given to potential sources for the procurement of comparable personnel, and to sources for copies of essential and critical documents to replace or reactivate the installation.

(c) **Location.** Consideration must be given to installation location and the effect surrounding elements have upon its security. The area may be highly industrial, congested residential, urban, or sparsely populated. The surrounding area may offer favorable natural cover to enemy espionage, terrorist, or sabotage agents. Consideration should also be given to the area's transportation facilities and to endemic natural hazards, such as flood, forest fires, or adjacent flammable storage areas.

(d) **Security Classification of Information.** A major factor in evaluating the sensitivity of an installation is the classification of the information stored, used, and generated there. Logically, information of greater importance to national

defense requires greater safeguarding from all standpoints. While regulations establish some safeguarding requirements, comparable measures, not specifically established by regulations, very likely are required in other areas. In considering the classification of information, the amount of classified information present must also be determined.

(e) Number of Like Installations. In determining the overall importance of an installation, consideration must be given to installations or activities capable of absorbing the functions of the surveyed installation to maintain mission continuity in the event the surveyed installation is neutralized or destroyed. If no other organization can assume these duties, the importance of the surveyed installation is greatly increased; however, the fact that similar installations or activities exist may not significantly lower the critical rating. Similar installations may not be in a position to absorb the mission of another, or if the mission is primarily devoted to a defined geographical area, there may be no substitution regardless of how many similar installations exist. In considering the substitution or replacement of an installation or the assumption of its mission, consideration must be given to the time involved. How long before the changeover or substitution can be effected? Can the alternate installation facilities achieve a comparable level of operating efficiency? If the alternate installation cannot operate at an acceptable level of efficiency, how long will it take to attain this desired level? Will this transition period affect the national defense effort to a great degree?

(f) Importance to the Defense Effort. In some instances, evaluation of the installation's importance may be made locally, based upon a joint effort between the survey team and the installation commander and his staff. Other knowledgeable persons within the installation and command, and the evaluation and correlation of available information from other agencies, adjacent commands, and from the agency utilizing the end product are also of prime importance. In most instances, this evaluation will be made at higher echelons of command. The basic consideration is the importance of the installation—its mission, functions, and production—to the national defense effort. The mission of the installation is a fairly good indicator of its importance; however, when the mission is compared with the cost of replacement, location of the installation, existence of similar installations able to absorb the operation of the surveyed installation, the overall importance of the surveyed installation may be higher or lower than anticipated. The survey team requires such information before determining the actual security needs of the particular installation. When the sensitivity rating is juxtaposed with the installation's current security situation, the survey team can offer recommendations to raise or lower the level of security on the installation in consonance with its sensitivity or importance to the national defense effort.

(g) Vulnerability to Terrorist Attack. An evaluation of the installation and its personnel as possible terrorist targets also must be made. This evaluation is based also on the elements listed in subparagraphs 402d(2)(a) through (f), and on the potential or known terrorist threat.

(3) Determination of Existing Security Measures. Once a determination of the relative degree of security required for the installation has been made, a detailed examination of the existing security situation is conducted. This examination includes all factors pertaining to document, personnel, and physical security measures. Examination techniques are dependent on the number of personnel available, personnel capabilities, time available, and choice. Security (document, personnel, and physical) may be examined separately at each location at different times. This is easier but more time-consuming than examining all types of security simultaneously at each location. If sufficient personnel are available, individuals or teams may be assigned to conduct separate portions of the survey; however, due to the interrelationships of security elements and areas, extensive coordination is required.

(a) Document Security. Document security is probably the most important part of the counterintelligence survey. It includes a systematic inspection of all security procedures used in the handling of classified documents, information, and other classfied material. Many aspects of document security may appear to be mechanical in nature; however, these may be misleading. Survey team personnel must visualize the security procedures employed from the viewpoint of an enemy agent in order to identify weaknesses and vulnerable areas in the system. A clear understanding of installation/unit organization is required to check the security and flow of classified information. The inflow of classified information generally starts at higher headquarters and flows down to lower echelons. The outflow of classified information usually follows the reverse pattern. Normally, all accounting records and security procedures for handling classified documents and material are examined at one level of command before moving to the next.

(b) Personnel Security. Personnel security includes the security clearance and education programs. Personnel security clearance procedures for the installation or unit must be carefully audited for the proper initiation, granting, recording, and termination of security clearances. In addition, the distinction between clearance level, access, and *need-to- know* is clearly emphasized in examining requirements for access to classified material. The security education program of the installation or unit is examined for completeness and effectiveness. Objectives of the security education program are to protect classified information and to instill a sense of security awareness in all personnel. The security education of an individual can be successful only when security is consciously accepted as a personal responsibility. Procedures for conducting required briefings/debriefings, as well as individual proficiency and attitudes toward security, provide an indication of the efficiency of the security education program.

(c) Physical Security. Physical security is distinct from document and personnel security as it comprises a system of controls, barriers, and other devices and procedures to prevent destruction, damage, and unauthorized access to installations and facilities. The overall physical security of an installation is the functional responsibility of the provost marshal; however, physical security measures which directly protect areas containing classified material, and critical areas susceptible to sabotage and terrorism, are of direct concern in conducting the counterintelligence survey. In addition, the overall physical security measures, plans, and procedures of the installation are evaluated as they relate to all aspects of counterintelligence. In the event that the installation/organization being surveyed has on record a physical security survey performed by the military police, a statement referring to the report and additional recommendations, if any, are sufficient. If there is no record of a previous survey, the provost marshal is contacted to schedule and coordinate, with the counterintelligence agency, the conduct of a physical security survey. When the installation is of the *open post* type with few physical restrictions directly related to counterintelligence security requirements, emphasis is on an examination of the physical security factors directly affecting classified storage areas, security areas, critical areas that require protection from sabotage, or terrorist attack, and other locations designated as sensitive.

(4) Recommendations. Based on the security requirements of the command and the existing security measures and procedures, recommendations are made to safeguard the installation/organization against espionage, sabotage, terrorism, and subversion. For each security hazard, there must be a reasonable recommendation for correction. In formulating realistic recommendations, consideration is given to cost, time, manpower, and availability of materiel. Alternate recommendations may be made to ensure corrective action if the primary recommendations cannot be implemented.

(5) Exit Briefing. Upon completion, and after preliminary formulation of the results and tentative recommendations, the commander and his

staff should be briefed on the survey. During this briefing, the findings and tentative recommendations are discussed. A successful briefing will, in most cases, ensure that the survey team's recommendations are realistic and can be implemented with minimum difficulty.

403. Counterintelligence Evaluation

Counterintelligence evaluations are similar to surveys, but limited in scope. An evaluation is normally conducted for a small unit or a component of a larger organization when there has been a change in the security posture, an activation or reactivation, or a physical relocation. Counterintelligence evaluations are normally limited to areas containing or processing classified material.

The counterintelligence evaluation may be limited to an assessment of only one type of security, such as document, personnel, or physical security, or it may include any combination, depending on the needs of the unit. The procedures for the preparation and conduct of the evaluation are the same as those for the counterintelligence survey; however, they usually are not as extensive. The counterintelligence evaluation also may be used to update counterintelligence surveys when only minor changes have occurred within an installation or major organization.

404. Counterintelligence Inspections

The counterintelligence inspection is performed to determine compliance with established security policies and procedures. The scope of the inspection will vary depending on its type and purpose. Inspections may include the following:

- Determination if assigned personnel with access to classified material are properly cleared.
- Determination if classified material is properly safeguarded by assigned personnel.
- Examination of facilities and containers used for storing classified material to determine adequacy.
- Examination of procedures for controlling entrances and exits, guard systems, and special guard instructions relating to security of classified material and sensitive areas.

Counterintelligence inspections include announced, unannounced, and penetration inspections. In addition to formal inspections, counterintelligence elements also maintain regular contact with all supported units to provide continuous informal assistance, support, and advice regarding security matters.

a. Announced Inspections. An announced inspection is one that has been publicized. All personnel concerned are aware of the inspection schedule and make preparations as necessary. Inspections are conducted on a recurring basis to ensure security standards remain at a high level. The announced inspection is often accomplished in conjunction with inspections conducted by the Inspector General and the commanding general.

b. Unannounced Inspections. The unannounced inspection is conducted to determine compliance with security policies and procedures at a time when special preparations have not been made. The unit or section to be inspected is not informed in advance of the inspection. The inspection may be conducted at any time during or after normal working hours. Counterintelligence personnel conducting unannounced inspections must have with them their credentials and authorization of the commander to conduct the inspection. In addition, a responsible person from the command should accompany the inspection team.

c. Penetration Inspections. A penetration inspection is designed to provide a realistic test of the security measures of an installation. The inspection is conducted in such a manner that installation personnel, other than the commander and those persons he desires

to notify, are unaware that such action is taking place. This type of inspection may be all-inclusive or may be limited to an attempt by counterintelligence personnel to fraudulently gain access to a specific sensitive area within the installation for the purpose of performing simulated espionage or sabotage acts. The simulated activities should be realistic and correspond to activities which might be attempted by a foreign power or hostile agent. The penetration inspection must be thoroughly planned and coordinated. Planning for the inspection includes consideration of the following:

- A responsible person from the inspected command, knowledgeable of the inspection, must be available at the installation during the inspection.
- Inspection personnel must carry a letter of identification and authorization to be used only in emergency situations.
- If at any time during the inspection a situation arises which would physically endanger personnel, the inspection is immediately terminated.
- The inspection must not impair or disrupt the activities of the command or installation unless that is specifically within inspection guidelines.
- Command or installation personnel must not be utilized in a manner that would tend to discredit them.

405. Technical Surveillance Countermeasures (TSCM) Support

Historically, hostile intelligence services have used technical surveillance monitoring systems in their espionage operations against U.S. installations, both in the United States and abroad. A technical surveillance monitoring system may be defined as any visual surveillance or audio monitoring system which is used clandestinely to obtain classified, or sensitive unclassified, information for intelligence purposes. These monitoring systems include, but are not limited to, the following:

- Sound pickup devices, such as microphones and other transducers which use wire and amplifying equipment.
- Passive modulators.
- Energy beams (i.e., electromagnetic, laser, and infrared).
- Radio transmitters.
- Recording equipment.
- Telephones (i.e., taps and bugs).
- Photographic and television cameras.

Normally, one Marine counterintelligence team assigned to each Marine amphibious force (MAF) maintains a TSCM capability to support tactical units of the MAF. This capability, designed primarily for combat support, also supplements the Naval Investigative Service (NIS) TSCM responsibilities during peacetime garrison conditions.

The purpose of the TSCM support program is to assist the commander in his overall security responsibilities by employing devices and techniques designed to locate, identify, and neutralize the effectiveness of hostile intelligence services technical surveillance activity. Technical surveillance countermeasures support consists of inspections and surveys. A TSCM inspection is an evaluation to determine the physical security measures required to protect an area against visual and audio surveillance; TSCM surveys include a complete electronic and physical search for unauthorized modification of equipment, the presence of clandestine audio and visual devices, and other conditions which may allow the unauthorized transmission of any conversation out of the area being surveyed. All TSCM operations are governed DOD Directive 5200.9, SECNAVINST 5500.31__, and MCO 05511.11__.

Requests for TSCM support must be classified and no conversation concerning the inspection should take place in the vicinity of the area to be inspected. Procedures for requesting inspections and surveys, TSCM responsibilities, and further information on the audio surveillance threat are contained in OPNAVINST 0500.46__ and MCO 05511.11__.

406. Reports

Sample formats for reports concerning counterintelligence surveys, inspections, and technical surveillance countermeasures support are contained in appendix B. Format for TSCM reports will be modified to meet the Naval Investigative Service requirements when supplementing the NIS effort.

Section 5

Counterintelligence Planning

501. General

Counterintelligence planning is accomplished concurrently with other intelligence and operational planning and continues until completion of the operation. All aspects of counterintelligence activities are considered to ensure adequate support for all phases of the operation. Counterintelligence plans become more detailed at each lower echelon, but remain flexible to respond to changing situations.

Counterintelligence activities are characterized by imaginative exploitation of all available resources. The counterintelligence effort focuses on the overall hostile intelligence collection, sabotage, terrorist, and subversive threat and is sufficiently flexible to adapt to the geographical environment, attitudes of the indigenous population, mission of the supported command, and changing emphasis by hostile intelligence, sabotage, terrorist, and subversive organizations.

Counterintelligence activities do not achieve maximum effectiveness when conducted separately from other intelligence activities. Counterintelligence activities must be integrated with the overall intelligence effort and be closely coordinated with activities of other intelligence specialist teams as well as with civil affairs, psychological operations, and similar organizations in contact with the indigenous population.

Counterintelligence participation and assistance is included early in the planning phase of tactical operations so that commanders benefit from counterintelligence information and assistance in the early formulation of tactical plans. Particular attention is directed towards identification of friendly vulnerabilities to be exploited

by hostile collection assets and toward recommendations for specific counterintelligence measures.

502. Planning Preceding the Operation

The effectiveness of counterintelligence operations in tactical areas depends largely upon the planning preceding the operation. The counterintelligence staff officer performs three separate functions in carrying out his planning responsibilities:

- Directs the effort to obtain information on the enemy's intelligence, sabotage, terrorism, and subversion capabilities.
- Provides for the production and dissemination of intelligence on the enemy's intelligence, sabotage, terrorism, and subversion capabilities, including clandestine and covert capabilities.
- Plans, recommends, and monitors counterintelligence measures throughout the entire command.

a. Collection and Processing of Information. The determination of requirements for information in counterintelligence planning, and the collection and processing of such information, follow the same procedures prescribed for other types of intelligence information. (See FMFM 2-1, *Intelligence*.) Especially pertinent to counterintelligence planning is information on every aspect of the enemy's intelligence system. Included are such matters as the hostile intelligence organization, means available to the enemy for the collection of information, and hostile sabotage, terrorism, and subversion agencies and capabilities.

b. Counterintelligence Estimate. Normally, a counterintelligence estimate is prepared by Fleet Marine Force (FMF) organizations having counterintelligence personnel assigned or attached. Forming the basis for the counterintelligence plan and appendix, the counterintelligence estimate includes the enemy's capabilities for intelligence, subversion, terrorism, and sabotage and the effects of the characteristics of the area on these capabilities and friendly counterintelligence measures. If a counterintelligence estimate is not prepared, the counterintelligence officer contributes to the preparation of the intelligence estimate, particularly subparagraphs on enemy intelligence, subversion, sabotage, guerrilla warfare, terrorism, and the effects of the characteristics of the area on these enemy capabilities. See appendix C for a sample format of a counterintelligence estimate.

c. Counterintelligence Measures Worksheet. Based upon the conclusions reached in the intelligence estimate of the enemy capabilities for intelligence, subversion, terrorist activities, and sabotage, the counterintelligence worksheet is prepared or revised. This worksheet is an essential aid in counterintelligence planning and is the basis for preparing counterintelligence orders and requests. See appendix D for an example of a counterintelligence measures worksheet.

d. Joint Operational Planning System (JOPS). Counterintelligence input to operation plans (counterintelligence and human intelligence (HUMINT) resources appendixes) will be in the current JOPS format (see app. E). The counterintelligence plan (see app. F) is no longer used as the counterintelligence appendix to the intelligence annex to operation plans. Nevertheless, the counterintelligence plan is a useful guide for planners at the Marine amphibious force (MAF) or higher level as a working paper. Selected elements of JOPS, Volume II may be integrated into the counterintelligence plan, as required.

503. Counterintelligence Targets

a. Selection and Priorities

(1) Counterintelligence targets include personalities, installations, and organizations of intelligence or counterintelligence interest which must be seized, exploited, or protected.

(2) The selection and assignment of targets is based on an assessment of the overall hostile threat and considers both the immediate and obvious threats to security as well as future threats. This assessment normally is conducted at the force level where the resultant counterintelligence target lists are also produced, and which include any counterintelligence targets assigned by higher headquarters.

(3) Numerical priority designations are assigned to each target to emphasize the relative importance and value of the target and/or to indicate the degree of security threat and urgency in neutralizing or exploiting the target. Priority designations established by higher headquarters are not altered; however, lower echelons may assign priorities to locally developed targets.

(4) Counterintelligence targets are usually assigned priority designations according to the following criteria:

(a) **Priority One.** Those targets representing the greatest security threat or possessing the largest potential source of intelligence or counterintelligence information/material and which must be exploited or neutralized as soon as possible.

(b) **Priority Two.** Those targets of lesser significance than priority one to be taken under control after priority one targets have been neutralized or exploited.

(c) **Priority Three.** Those targets of lesser significance than priority one or two to be neutralized or exploited as time and personnel permit.

b. Personalities. Except for well-known personalities, most persons of counterintelligence interest are identified and developed by counterintelligence units once operations are established ashore. Personalities are divided into three categories comprising those persons who are a threat to security, whose intentions are unknown, and who can assist the intelligence and counterintelligence effort. For ease in identification, a color code indicates the categories.

(1) **Black List.** Black lists, developed or compiled at all echelons of command, contain the identities and locations of individuals considered to be a threat to security and whose capture and detention are of prime importance. The black list includes the following persons:

- Known or suspected enemy or hostile espionage, sabotage, terrorist, political, and subversive individuals.
- Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.
- Political leaders known or suspected to be hostile to the military and political objectives of the United States and/or an allied nation.
- Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to the U.S. forces.
- Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to the U.S. forces.
- Known enemy military or civilian personnel who have engaged in intelligence, counterintelligence, security, police, or political indoctrination activities among troops or civilians.
- Other enemy personalities indicated by the G-2, such as local political personalities, police chiefs, and heads of significant municipal and/or national departments or agencies.

(2) **Gray List.** Gray lists, compiled or developed at all echelons of command, contain the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the United States are obscure. Regardless of their leanings, personalities may be on gray lists when known to possess information or particular skills required by U.S. forces. They may be individuals whose political motivations require further exploration before they can be utilized effectively by U.S. forces. Examples of individuals who may be included in this category are:

- Potential or actual defectors from the hostile cause whose credibility has not been established.

- Individuals who have resisted, or are believed to have resisted, the enemy government and who may be willing to cooperate with U.S. forces, but whose credibility has not been established.

- Nuclear scientists, physicists, and technicians suspected of having been engaged in enemy nuclear research projects or nuclear missile programs against their will.

(3) White Lists. White lists, compiled or developed at all echelons of command, contain the identities and locations of individuals in enemy-controlled areas who are of intelligence or counterintelligence interest and are expected to be able to provide information or assistance in the accumulation of intelligence data or in the exploitation of existing or new intelligence areas of interest. They are usually in accord with or favorably inclined toward U.S. policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation, critical need for specialists in scientific fields, and such intelligence needs as are indicated from time to time. Examples of individuals included in this category are:

- Former political leaders of a hostile state deposed by the hostile political leaders.

- Intelligence agents employed by U.S. or Allied intelligence agencies.

- Key civilians in areas of scientific research, to include faculty members of universities and staffs of industrial or national research facilities whose credibility has been established.

- Leaders of religious groups and other humanitarian groups.

- Other persons who can significantly aid the political, scientific, and military objectives of the U.S. and whose credibility has been established.

c. Installations. The installation target is any installation, building, office, or field position that may contain information or material of counterintelligence interest or which may pose a threat to the security of the command. Examples of installation type targets are as follows:

- Installations formerly or currently occupied by enemy espionage, sabotage, and subversive agencies or enemy police organizations, including prisons and detention centers.

- Installations occupied by enemy intelligence, counterintelligence, security, or paramilitary organizations, including operational bases, schools, and training sites.

- Enemy communication media and signal communication centers.

- Nuclear research centers and chemical laboratories.

- Enemy political administrative headquarters.

- Production facilities, supply areas, and other installations to be taken under control to deny support to hostile guerrilla and partisan elements.

- Public utilities and other installations to be taken under early control to prevent sabotage. These installations are usually necessary for the rehabilitation of civil areas under U.S. control.

- Embassies and consulates of hostile governments.

d. Organizations. Any organization or group which is an actual or potential threat to the security of U.S. or Allied forces must be neutralized. The threat an organization or group presents may not be immediately apparent to the military commander, intelligence officer, or counterintelligence unit. The enemy frequently camouflages his espionage or subversive activities with the establishment of front organizations or groups which, if permitted to remain in being, could impede the success of the military operations. Examples

of hostile organizations and groups which are of major concern to the counterintelligence unit during tactical operations include:

- Hostile intelligence, sabotage, subversive, and insurgent organizations or groups.
- National and local political groups and parties known or suspected to have aims, beliefs, or ideologies contrary or in opposition to those of the United States.
- Paramilitary organizations, including student, police, militia/veterans, and excombatant groups, known to be hostile to the United States.
- Hostile sponsored groups and organizations whose objectives are to create dissension and spread unrest among the civilian population in the area of operations.

504. Counterintelligence Target Reduction

The timely seizure and exploitation of counterintelligence targets requires a detailed and well-coordinated counterintelligence reduction plan prepared well in advance. The reduction plan must be kept current.

All targets, assigned or developed, located within the unit's area of operation are listed in the reduction plan. Counterintelligence elements supporting tactical assault units normally prepare the reduction plan based on the scheme of maneuver with the targets listed in the sequence in which they are expected to appear in the area of operation. The target priority designations, however, remain as assigned on the counterintelligence target list, with highest priority targets covered first when more than one target is located in the same general area. Neutralized and exploited targets are deleted from the counterintelligence reduction plan and appropriate reports are submitted.

A well-prepared and comprehensive counterintelligence reduction plan ensures coverage of all significant counterintelligence targets and allows all counterintelligence units to conduct daily operations based on established priorities. Appendix F contains a sample counterintelligence reduction plan.

505. Sequence of Counterintelligence Activities for Amphibious Operations

Counterintelligence functions fall into a logical sequence corresponding to the five phases of an amphibious operation and into required actions in the postoperation period. The following outline of counterintelligence activities is provided as a guide for intelligence and counterintelligence officers in planning for amphibious operations:

a. Amphibious Operations

(1) Planning Phase

(a) Provide assistance to the command operations security program. During the initial planning phase, counterintelligence assets provide assistance to the G-3/S-3 in establishment of the operations security program.

(b) Planning information is released only on a *need-to-know* basis. Common sense is required to determine the size and composition of the *need-to-know* group. It may be necessary to initiate action to obtain clearances for certain members of the command.

(c) All material referring to the operation is given appropriate security classification. Guidance ensures that particularly sensitive items are identified and restricted from being carried forward of battalion command posts or in aircraft flying over enemy held terrain.

(d) Determine if code symbols are necessary for marking of vehicles and operational equipment; if so, they are used to cover existing tactical marking.

(e) Avoid compromising activities. Special innoculations or the issuance of special clothing and equipment should be postponed until after embarkation, when possible. Leave and liberty are reduced gradually, since any sudden curtailment will engender speculation.

(f) The Wartime Information Security Program (WISP) is stressed constantly. Individual self-censorship is emphasized as this is the only effective censorship program. Also, possession of diaries is normally forbidden, and personal cameras are rigidly controlled.

(g) Prepare the HUMINT and counterintelligence appendixes for issuance as part of the intelligence annex.

(h) To minimize the probability of later compromise, recommendations should be submitted on the selection of embarkation and rehearsal areas, routes, and times for the movement to the embarkation areas.

(i) The importance of these measures can be appreciated when the unique opportunities for espionage during the planning phase are understood. The nature and extent of friendly activities, offering widespread opportunity for information collection, cause information on the operation to be most susceptible to compromise during this phase, unless properly protected.

(2) Embarkation Phase

(a) Establish liaison with other counterintelligence agencies to ensure control of civilians in the embarkation area and along the routes to that area. Civilians working in the embarkation area are screened prior to employment.

(b) Ensure that contact between troops and civilians en route and in the embarkation area is kept to an absolute minimum.

(c) Establish security over the embarkation area to prevent espionage and sabotage.

(d) Ensure positive identification of all persons to be embarked.

(e) Due to the necessity to transport and marshal large amounts of equipment, the threat of sabotage is at its height during the embarkation phase. Proper measures are necessary to deny the enemy access to the many potentially lucrative targets.

(3) Rehearsal Phase

(a) If the rehearsal area is close to possible civilian observation, patrols are placed ashore to seal off the rehearsal area. Similarly, the amphibious task force (ATF) seals off the rehearsal area from sea and air observation.

(b) In coordination with the communication officer, communication security is emphasized. Transmission power should be reduced to the minimum required, and frequencies and call signs should not be those intended for actual operational use.

(4) Movement Phase

(a) Remove restrictions on informing the troops about D-day, H-hour, designated landing beaches, helicopter landing zones, selected objective and force beachhead, and the mission.

(b) Impose WISP if directed.

(c) In coordination with the communication officer and subordinate commanders, provide assistance in the maintenance of communications security within units of the landing force.

(5) Assault Phase. Supervise the accomplishment of counterintelligence operations in accordance with the counterintelligence plan. Included are the following:

(a) Contact local authorities and persons known to be friendly to collect all available counterintelligence information and to screen local inhabitants.

(b) Establish security against sabotage or terrorism for all military installations and those civilian installations to be kept in operation.

(c) Establish a counterintelligence interrogation center adjacent to the prisoner-of-war interrogation center or other secure area.

(d) Establish civilian control measures such as checkpoints, identification cards, and curfews in coordination with the personnel officer.

(e) Locate and recover contraband materiels, such as arms, explosives, communication equipment, food, medical supplies, or other items not surrendered in accordance with proclamations.

(f) Enforce camouflage and blackout regulations.

(g) Publish effective countersigns.

(h) Conduct security checks of all areas vacated by our troops, particularly command posts, to determine if any compromising material has been inadvertently left behind.

(i) Establish counterreconnaissance measures in coordination with the operations officer.

(j) Seize, exploit, and protect counterintelligence targets.

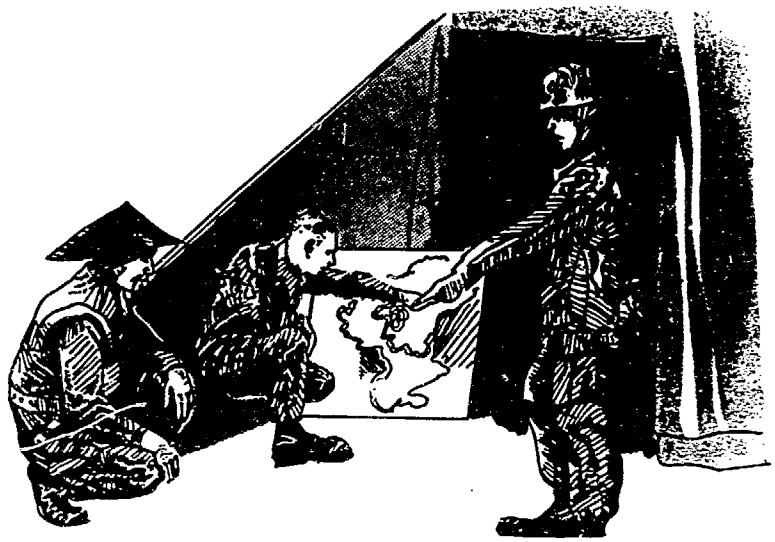
b. Postoperation Period

(1) Complete studies of the enemy organization, weapons and equipment, techniques, and effectiveness in conducting intelligence, subversion, terrorism, and sabotage operations.

(2) Submit appropriate reports on observed or investigated civilians.

(3) Evaluate and report the effectiveness of the counterintelligence teams, techniques and procedures, and equipment employed.

(4) Evaluate and report the effectiveness of counterintelligence operations.



Section 6

Counterintelligence Training

601. General

Counterintelligence training is integrated with other intelligence training and the command training program. All personnel receive training in counterintelligence and security as a basis for fulfilling basic responsibilities in safeguarding information of value to the enemy or a potential enemy. Intelligence and counterintelligence personnel receive additional training to improve their proficiency in accomplishing the intelligence and counterintelligence mission.

602. Responsibilities

Counterintelligence and security training is the responsibility of the commander. This responsibility is not limited to units with assigned counterintelligence or intelligence personnel, but extends also to commanders of smaller units. The intelligence officer is responsible to the commander for the planning and supervision of inteiligence and counterintelligence training of his own section and, in coordination with the operations officer, exercises staff supervision over intelligence and counterintelligence training within the entire command. The staff counterintelligence officer monitors the counterintelligence and security training programs of the command and advises and assists the intelligence officer in performing his counterintelligence training responsibilities. Counterintelligence team commanders are responsible for the training of team personnel.

603. Purpose and Scope

The ultimate objective of counterintelligence training is to ensure effective contribution by all personnel to the

counterintelligence effort and to instill a sense of security discipline. The effectiveness of command counterintelligence and security measures often rests on the individual Marine's ability to recognize and accurately report threats to the security of the command and his willing acceptance of a high degree of security discipline. Basic counterintelligence and security training requirements are common to all commands; however, emphasis on certain subjects will vary according to the mission of the command and duty assignments of personnel with the unit. Generally, training can be divided into the following categories:

- Basic counterintelligence and security training for all personnel.
- Training for officers and staff noncommissioned officers.
- Training for intelligence personnel.
- Training for counterintelligence teams.

604. Basic Counterintelligence and Security Training

a. Counterintelligence and Security Subjects. All officers and enlisted personnel should receive training in the following counterintelligence and security subjects:

- Protection of classified material and other information which may be of value to an enemy.
- Troop movement security measures.
- Wartime Information Security Program (WISP).
- Defense against hostile espionage, subversion, terrorism, and sabotage.
- Actions in the event of possible espionage, subversion, terrorism, or sabotage.
- Use of countersigns.
- Purpose, scope, and organization of Marine Corps counterintelligence.

b. Related Subjects. All officers and enlisted personnel should receive training in the following related subjects:

- Camouflage.
- Survival, evasion, resistance to interrogation, escape, and the U.S. Code of Conduct.
- Rights and responsibilities under the Geneva Convention of 12 August 1949.

605. Training of Officers and Staff Noncommissioned Officers

The following subjects are considered appropriate for additional counterintelligence training of officers and staff noncommissioned officers:

- Functions, capabilities, limitations, and employment of counterintelligence teams.
- Counterintellience operations and security measures.
- Organization, methods of operation, and intelligence collection capabilities of hostile intelligence organizations in areas of probable operations.
- Identification, control, and reporting of persons and installations of counterintelligence interest.
- Implementation, operation, and responsibilities of WISP.

606. Training of Intelligence Section Personnel

The following additional subjects are considered appropriate for the counterintelligence training of intelligence section personnel:

- Intelligence collection capabilities of counterintelligence teams.

- Counterintelligence sources of information and methods of reporting.
- Counterintelligence operations and security measures.

607. Training of Counterintelligence Team Personnel

a. Essential Subjects Training. Counterintelligence team personnel are subject to essential military subjects training designed to maintain their basic military proficiency. In addition, in order to maintain a high degree of proficiency, expertise, and professionalism in accomplishing the counterintelligence mission, counterintelligence teams conduct an active training program which includes the following subjects:

(1) General Subjects

(a) Appropriate aspects of the mission, task organization, and concept of operations of the command to which attached

(b) Hostile intelligence organizations in the area of probable operations, to include organization, methods of operation, schools and training, capabilities, limitations, communications, and personalities.

(c) History, geography, and political, social, and ethnic factors in the area of probable operations.

(d) Customs, habits, and commonly used expressions of the populace in the area of probable operations.

(e) Friendly and hostile underground, political, or paramilitary organizations or groups in the area of operations.

(f) Security and law enforcement agencies in the area of operations and the methods of population control.

(g) Hostile ground, air, and naval organizations, tactics, and techniques.

(h) Hostile weapons, documents, maps, and overlays.

(i) Hostile communication systems and equipment in the area of probable operations.

(j) Visual recognition of key persons of counterintelligence interest believed to be in the target areas, utilizing photographs, written descriptions, or identifying characteristics based on all obtainable information.

(k) U.S. and allied intelligence, counterintelligence, and security organizations including their functions, capabilities, and limitations.

(l) International terrorist organizations, personalities, and methods of operation.

(2) Intelligence Subjects

(a) Order of battle analysis.

(b) Photo imagery interpretation.

(c) Battlefield surveillance planning and analysis.

(d) Preparation of intelligence studies, such as beach and helicopter landing site studies, town plans, and road and trail net studies.

(e) Maintenance of enemy situation maps.

(f) Intelligence and counterintelligence aspects of tactical cover and deception operations.

(g) Principles of the intelligence cycle and the integration of counterintelligence.

(h) Additional intelligence subjects as contained in FMFM 2-1, *Intelligence*.

(3) Counterintelligence Planning and Operations

(a) Determination of requirements for the collection of the information necessary for

counterintelligence planning, to include sources of information and the intelligence collection plan.

(b) Preparation of counterintelligence estimates, plans, worksheets, target lists, and reduction plans.

(c) Evaluation, selection, exploitation, and neutralization of counterintelligence targets.

(d) Planning, preparation, coordination, and conduct of special operations, including counterespionage, countersubversion, counterterrorism, and countersabotage operations.

(e) Planning, preparation, coordination, and conduct of screening operations and troop movement security.

(f) Principles and techniques of interrogation with and without the use of an interpreter.

(g) Investigation of espionage, sabotage, subversion, terrorism, and defection to include principles, techniques, handling of evidence, and legal principles.

(h) Planning, preparation, and conduct of counterintelligence surveys, evaluations, and inspections.

(i) Planning, selection, and control of human intelligence sources.

(j) Investigation and debriefing of U.S. personnel listed as captured, missing (nonhostile), and missing in action.

(k) Planning, implementation, and conduct of WISP operations.

(l) Maintenance of counterintelligence files and preparation of reports.

(m) Techniques for the handling, treatment, and control of enemy personnel captured or detained, and the handling of captured documents and equipment. Training includes applicable provisions of the Geneva Conventions.

(n) Establishing and maintaining liaison to include methods, types of organization/agencies, and benefits derived.

(o) Foreign language training to maintain and enhance language capabilities.

(4) Technical Training

(a) Defense against methods of entry and technical surveillance devices. Training in defense against technical surveillance devices is generally limited to the threat, types of clandestine listening devices, and protective measures, except for those teams that have a technical surveillance countermeasure (TSCM) capability where training is more extensive.

(b) Principles and techniques of photography and defense against clandestine photography.

(c) Chemical, mechanical, and electronic investigative aids.

(d) Sabotage and terrorist devices and techniques.

(e) Operation and maintenance of team communication equipment.

(f) Operation and first echelon maintenance of team ordnance and motor transport equipment.

(g) Marine Air-Ground Intelligence System/Joint Interoperability of Tactical Command and Control Systems (MAGIS/JINTACCS).

(5) General Military Subjects

(a) Map reading to include map tracking, overlays, and use of the compass.

(b) Weapons training to include small arms, grenade launchers, and machineguns.

(c) Mines and boobytraps, including detection, emplacement, neutralization, and fabrication.

(d) Offensive and defensive tactics and retrograde movements. Training includes amphibious and helicopterborne operations, scouting and patrolling, ambushes, and raids.

b. Field Training Exercises. Counterintelligence teams participate to the maximum extent possible in field training exercises to maintain and improve proficiency in counterintelligence planning, coordination, operations, and tactical concepts. To obtain maximum benefit from such training, the following aspects must be considered:

(1) Counterintelligence personnel are assigned to the exercise planning staff to conduct counterintelligence planning and ensure realistic counterintelligence activity during the exercise.

(2) Complete counterintelligence planning is conducted to include counterintelligence estimates, plans, target lists, and reduction plans.

(3) Hostile intelligence activity must be included which will require the widest range of counterintelligence operations.

(4) Actors are used to the maximum extent possible to add realism to counterintelligence operations. Often, personnel with a foreign language capability and interrogator-translator personnel can be used effectively as actors for specific counterintelligence activities.

(5) In addition to conducting the widest range of counterintelligence operations, the exercise includes, whenever possible, the attachment and detachment of subteams, movement of the team headquarters, and situations to test the adequacy of team control and communications.

Appendix A

Format for Personnel Data Form, Persons Captured, Missing (Nonhostile), or Missing in Action

1. PERSONAL DATA:
   a. NAME:
   b. RANK:
   c. SSN/MOS:
   d. FORMER SERVICE NUMBER:
   e. ORGANIZATION:
   f. DATE OF BIRTH:
   g. PLACE OF BIRTH:
   h. HOME OF RECORD:
   i. RESIDENCE (If other than home of record):
   j. MARITAL STATUS (Include number, sex, citizen status, and age of children):
   k. PEBD:
   l. EAS/EOS:
   m. DATE ARRIVED IN COUNTRY:
   n. DUTY ASSIGNMENT:

2. PHYSICAL CHARACTERISTICS:
   a. HEIGHT (Metric as well as U.S. equivalent):
   b. WEIGHT (Metric as well as U.S. equivalent):
   c. BUILD:
   d. HAIR:
   e. EYES:
   f. COMPLEXION:
   g. RACE:
   h. RIGHT/LEFT HANDED:

3. DISTINGUISHING CHARACTERISTICS:

a. SPEECH (Include accent and speech patterns used):

b. MANNERISMS:

c. SCARS/IDENTIFYING MARKS (Include type, location, size, color, and detailed description):

d. OTHERS:

4. CIRCUMSTANCES OF INCIDENT:

a. DATE:

b. LOCATION (Coordinates and geographic name):

c. CIRCUMSTANCES:

d. REPORTED WOUNDS:

e. LAST KNOWN LOCATION:

f. LAST KNOWN DIRECTION OF TRAVEL:

g. LAST KNOWN PLACE OF DETENTION:

h. STATUS (Prisoner-of-war/missing [nonhostile]/missing in action as reported by unit):

5. OTHER PERTINENT DATA:

a. GENERAL PHYSICAL CONDITION:

b. LINGUISTIC CAPABILITIES AND FLUENCY:

c. RELIGION:

d. CIVILIAN EDUCATION:

e. MILITARY SCHOOLS:

f. CLOTHING AND EQUIPMENT WHEN LAST SEEN:

g. JEWELRY WHEN LAST SEEN (Include description of glasses, rings, watches, religious medalions, etc.):

h. OTHER PERSONNEL LISTED PW/MIA/MIS DURING SAME INCIDENT:

6. PHOTOGRAPH:

7. HANDWRITING SAMPLES

(Attach sample of correspondence, notes, etc. If no other sample is available, include reproduction of signature from SRB/OQR.)

ENCLOSURES: (May not be given wide dissemination based on classification or content.)

a. CLEARANCE/ACCESS INFORMATION. (Include information concerning security clearance, access, knowledge of recurring tactical operations, knowledge of projected or proposed operations, or any other special knowledge possessed.)

b. MEDICAL PROFILE. (Include pertinent information extracted from medical records and summarized information gained concerning ability to survive in captivity, known personal problems, relationship with seniors/contemporaries or other personal, medical, or personality information which would indicate his ability to cope in a prisoner-of-war situation.)

c. REFERENCES. (List any messages, letters, or other correspondence pertaining to the individual. If circumstances under which the individual is listed as captured or missing predicated a command investigation, a copy of that investigation is included as an enclosure.)

d. UNRESOLVED LEADS/INVESTIGATORS COMMENTS. (Include unresolved leads or names of personnel who were unavailable for interview because of transfer, evacuation, etc. Use investigator's comments as necessary but do not recommend a casualty determination.)

Appendix B

Counterintelligence Reports

1. SAMPLE FORMAT FOR COUNTERINTELLIGENCE SPOT REPORT

CLASSIFICATION

COUNTERINTELLIGENCE SPOT REPORT

This is an unevaluated Field Report

Report Number _____ Date/Time (Z) _____

FROM:
TO:

1. WHAT: _____

2. WHO: _____

3. WHERE: _____

4. WHEN: _____

5. DETAILS: _____

_____

_____

6. SOURCE: _____

7. RELIABILITY: _____

8. REMARKS: _____

_____

_____

Prepared By:

Approved By:

CLASSIFICATION

2. SAMPLE FORMAT FOR COUNTERINTELLIGENCE INFORMATION REPORT

CLASSIFICATION

COUNTERINTELLIGENCE INFORMATION REPORT

COUNTRY: REPORT NO:

TITLE:

DATE OF INFO: REPORT DATE:

ORIGINATOR: REFERENCES:

SOURCE:

SUMMARY:

DETAILS:

SOURCE COMMENT:

ORIGINATORS COMMENT:

PREPARED BY:

APPROVED BY: REQUEST EVALUATION ____Y ____N
REQUEST EVALUATION RELEASABLE TO:

____ ENCLOSURES(S):

DISTRIBUTION

CLASSIFICATION

Note: Evaluation of Source and Information

1. Determination of Reliability. In order to determine reliability of the source, the original source and reporting agency must be considered. Prisoners of war, for example, may or may not be reliable sources of information depending upon their national psychology and other factors. Information from indigenous personnel, even from those who are friendly, may be influenced by fear, confusion, the desire to please, or lack of perception on the part of the individual. Past performance of individual sources and reporting agencies is the best basis for judging reliability. An additional test of source and agency reliability is a consideration of whether, under the conditions existing at the time, the information could have been obtained.

2. Determination of Accuracy. An indication of information accuracy may be revealed by considering the degree that the information, based purely on logic, appears to be true. Accuracy is evaluated by examining the consistency of the information, and by comparing it with other information, particularly that known to be true, to confirm or corroborate its value. The most reliable method of judging accuracy is comparison with other information. Where possible, the collection effort seeks to obtain the same information through several sources and agencies.

3. Evaluation Rating System

a. Evaluation of information is determined by using a standard system; a letter is used to show the evaluation of reliability and a numeral to show the evaluation of accuracy.

b. Evaluation of the reliability of the source is shown as follows:

A – Completely reliable
B – Usually reliable.
C – Fairly reliable.
D – Not usually reliable.
E – Unreliable.
F – Reliability cannot be judged.

(1) If the source is a friendly informed person, A is assigned only when he is known to have a long experience and extensive background with the type of information reported. B is assigned to friendly informed persons who lack the background experience, but are of known integrity. F is assigned when there is no adequate basis for estimating the reliability of the source. This is true of captured enemy personnel and documents, particularly in the early days of an operation.

(2) Agencies are ordinarily rated A, B, or C, depending on their state of training and experience.

(3) When the source of an item and a collecting agency are evaluated differently, only the lower degree of reliability is indicated.

(4) The organization closest to the source or agency is normally the best judge of reliability. Consequently, higher headquarters generally accepts the reliability evaluation of the lower organization, and considers only the reliability of the reporting unit.

c. Evaluation of information accuracy is rated as follows:

1 – Confirmed by other sources.
2 – Probably true.
3 – Possibly true.
4 – Doubtful.
5 – Improbable.
6 – Truth cannot be judged.

(1) Confirmed by Other Sources. If it can be stated with certainty that reported information originates from a source other than that for already existing information on the same subject, it is classified as *confirmed* by other sources and is rated 1.

(2) Probably True. If, under the criteria above, no proof can be established, and if there is no reason to suspect that the reported information comes from the same source as the information already available on the subject, it is classified *probably*

true and is rated 2. If some report contents are confirmed by information already available, the above rating will also apply to unconfirmed information contained in the report.

(3) Possibly True. If the investigation reveals that the reported facts, on which no further information is yet available, comply with behavior of the enemy as observed up to now, the information received is *possibly true* and rated 3.

(4) Doubtful. Reported but unconfirmed information, the contents of which contradict estimated development or known behavior of the enemy, is classified *doubtful* and rated 4, as long as such information cannot be disproved by available facts.

(5) Improbable. Reported information, unconfirmed by available data and contradicting experience, is classified as *improbable* and is rated category 5. The same classification is given to reported information which contradicts existing data previously rated 1 or 2.

(6) Truth Cannot be Judged. If investigation of a report reveals that a basis for allocating ratings 1 to 5 is not present, the reported information is classified *truth cannot be judged* and rated 6. The statement that a report cannot be judged as to accuracy must always be preferred to an inaccurate use of the ratings 1 to 5; however, the possibility of a rating of 1 or 2 should always be tested. If such a rating is not possible because of lack of other information on the same target, the rating 6 has to be given.

d. Both a letter and a numeral designate the evaluation of a given item of information. Evaluations as to reliability and accuracy, however, are completely independent of each other. For instance, a highly reliable source may report an item which, when related to other information known to be true, appears to be improbable. Evaluation would be A-5. Conversely, an evaluation of E-1 would be given to an item of information from a source of known unreliability when, through confirmation by other sources, the information was of proven accuracy. A report disseminated to higher, lower, and adjacent units contains the evaluation for each item of information.

3. SAMPLE FORMAT FOR COUNTERINTELLIGENCE INTERROGATION REPORT

CLASSIFICATION

COUNTERINTELLIGENCE INTERROGATION REPORT

1. Preparing Unit/Team:

2. References: (Include ITU report if applicable.)

3. Enclosures:

4. Report Number: (Numbered sequentially by calendar year.)

5. Data/Time of Report (Z)

6. Date/Place: (Date and place of interrogation.)

MAP REFERENCE:

LANGUAGE USED: (During interrogation.)

NAME OF INTERPRETER:

CATEGORY AND CI INTEREST: (Category of subject – A, B, C, or D (see note below). State reason subject is of counterintelligence interest.)

PART I – PERSONAL DATA:

Name: (Surname, first, middle)

Aliases:

Rank/Position or Occupation:

Date of Birth: (Day/month/year)

Place of Birth:

Nationality: Race:

Height: Weight: Color Eyes: Color Hair:

Outstanding Identifying Features: (Scars, etc.)

Languages: (Include proficiency)

Unit/Organization/Address:

Family Data: (Identification of parents, spouse, children)

Career: (Summarize education, employment, etc.)

Military Experience:

Specialist Knowledge: (Knowledge of technical subjects or equipment)

CLASSIFICATION

CLASSIFICATION

PART II – CAPTURE INFORMATION:

Date/Time of Capture/Apprehension:

Capturing/Apprehending Unit:

Place and Circumstances of Capture/Apprehension:

Documents: (Carried at time of capture/apprehension, including money or other valuables)

Equipment: (Of intelligence interest, personal equipment/weapons)

PART III – INFORMATION OBTAINED:

PART IV – FILE INFORMATION:

(Report information on file which pertains to the subject or the information obtained.)

PART V – INTERROGATOR'S REMARKS:

(Interrogator's remarks are essential for second/followup interrogations at higher headquarters. Remarks should be as detailed as possible and include:)

(1) Assessment of Source: (Include source's experience, intelligence, cooperation, and attitude. State whether discrepancies were noted through use of control or repeat questions.)

(2) Discussion of Interrogation Technique: (State technique/orchestration under which source cooperated. Provide details of technique employment.)

(3) Recommendation for Further Interrogation: (State whether source is recommended for further interrogation and his specific areas of knowledge. *Note:* Recommendation should be consistent with category and counterintelligence interest code assigned to source.)

(4) Additional Remarks:

PART VI – DISPOSITION:

(State subject's present status and location. If to be moved, give approximate date and place of movement.)

PREPARED BY:

APPROVED BY:

CLASSIFICATION

Note: The following categories are used to describe the prisoner's intelligence potential:

A — High-level prisoner whose broad and specific knowledge of the war effort singles him for interrogation without delay by specially qualified interrogators at the highest level (i.e., general officers, scientists, political and intelligence officers, etc.).

B — Prisoner with enough information about the enemy or any subject of intelligence value, in addition to information of tactical value, to warrant further interrogation.

C — Prisoner with information of immediate tactical value unwarranting further interrogation.

D — Prisoner of no intelligence value.

4. SAMPLE FORMAT FOR COUNTERINTELLIGENCE AFTER-ACTION REPORT

CLASSIFICATION

COUNTERINTELLIGENCE AFTER-ACTION REPORT

1. Subject: (Type of operation and location)

2. Preparing Unit/Team:

3. Reference:

4. Report Number: (Numbered sequentially by calendar year.)

5. Date of Report:

MAP REFERENCE:

DETAILS:

a. Date/Time of Operation

b. Counterintelligence Unit Employed

c. Unit Supported

d. Summary of Operation

(Briefly describe the operation and the results.)

e. Recommendations for Future Operations

(Identify problems and recommendations for corrective action and/or indicate successful method and procedures that should be included in future operations.)

DISTRIBUTION

PREPARED BY:

APPROVED BY:

CLASSIFICATION

5. SAMPLE FORMAT FOR INVESTIGATION REPORT

COUNTERINTELLIGENCE REPORT (3850)
NAVMC 10481 (REV. 6-68)
Previous editions will not be used.

FILE NO. Control number
DATE Date report signed

CLASSIFICATION

SUBJECT Complete identification of person, organization, or incident	REPORTING ORGANIZATION Complete organization identification and address
REFERENCES List pertinent references	DISTRIBUTION OF REPORT List organizations/agencies receiving copies of the report
	_____ORIGIN OF REPORT Unit requesting/authority
ENCLOSURES List in order of report appearance	CASE CHARACTER/CATEGORY Type of investigation, espionage, subversion, terrorism, sabotage, etc.
	PERIOD COVERED Inclusive dates of investigation
	STATUS Closed/pending/referred/suspended, etc.

SYNOPSIS
(Summary of the report.)

1. PREDICATION: (How the investigation was initiated.)

2. PURPOSE: (Why the investigation was conducted and what was to be determined. State any limitations placed on the investigation.)

3. BACKGROUND: (Additional information which initiated the investigation and/or information concerning previous investigations or reported information of the subject. Also identify persons conducting the investigation.)

4. RESULTS: (Detailed information obtained during the investigation, usually in chronological sequence. The investigation steps initiated, interviews/interrogation, leads developed, and information derived.)

5. COMMENTS: (Comments of the investigator to aid reviewing personnel in the study and evaluation of the report. Only comments of the investigator are contained in this paragraph. All information obtained is reported under results.)

End of Report

CLASSIFICATION

REPORTED BY (Signature) Typed name of the senior person conducting the investigation and signature	APPROVED BY (Signature) Typed name and title of approving authority and signature

6. SAMPLE FORMAT FOR COUNTERINTELLIGENCE SURVEY REPORT

COUNTERINTELLIGENCE REPORT (3850)
NAVMC 10481 (REV. 6-68)
Previous editions will not be used.

FILE NO. Control number
DATE Date report signed

CLASSIFICATION

SUBJECT Counterintelligence Survey Unit Parent Organization Location	REPORTING ORGANIZATION Complete organization identification and address
REFERENCES List pertinent references	DISTRIBUTION OF REPORT List organizations/agencies receiving copies of the report
	_____ ORIGIN OF REPORT Unit requesting/authority
ENCLOSURES List in order of report appearance	CASE CHARACTER/CATEGORY Counterintelligence Survey
	PERIOD COVERED Inclusive dates of survey
	STATUS Closed/pending/referred/suspended

SYNOPSIS (Concise summary of the report.)

1. PREDICATION: (How the survey was initiated.)

2. PURPOSE: (What the survey was to determine and any limitations placed on the survey.)

3. BACKGROUND:

   a. Persons Conducting Survey

   b. Previous Surveys

   c. Mission

   d. Inherent Hazards of the Area

   e. Degree of Security Required. (Maximum, medium, or minimum based on following factors:)

      (1) Mission
      (2) Cost of replacement
      (3) Location
      (4) Number of like installations
      (5) Classified material
      (6) Importance

CLASSIFICATION

4. RESULTS:

   a. Security of Information

   b. Security of Personnel

   c. Physical Security

5. RECOMMENDATIONS: (List recommendations to correct security hazards as they appear in paragraph 4 under the subparagraph heading. Reference paragraph for clarity.)

   a. Security of Information

   b. Security of Personnel

   c. Physical Security

(*Note:* When a survey is conducted on a large command, it may be necessary to report the results and recommendations by sections within the command or by subordinate units.)

End of Report

CLASSIFICATION

REPORTED BY (Signature) Typed name of the senior person conducting the investigation and signature	APPROVED BY (Signature) Typed name and title of approving authority and signature

7. SAMPLE FORMAT FOR COUNTERINTELLIGENCE EVALUATION REPORT

COUNTERINTELLIGENCE REPORT (3850)
NAVMC 10481 (REV. 6-68)
Previous editions will not be used.

FILE NO. Control number
DATE Date report signed

CLASSIFICATION

SUBJECT Counterintelligence Evaluation (Personnel, Document, or Physical Security) Unit Parent Organization Location	REPORTING ORGANIZATION Complete organization identification and address
REFERENCES List pertinent references	DISTRIBUTION OF REPORT List organizations/agencies receiving copies of the report
	_____ ORIGIN OF REPORT Unit requesting/authority
ENCLOSURES List in order of report appearance	CASE CHARACTER/CATEGORY Counterintelligence Evaluation
	PERIOD COVERED Inclusive dates of evaluation
	STATUS Closed/pending/referred/suspended

SYNOPSIS (Concise summary of the report.)

1. PREDICATION: (How the evaluation was initiated.)
2. PURPOSE: (What the evaluation was to determine and any limitations placed on the evaluation.)
3. BACKGROUND: (Information on previous evaluations or surveys and information on amount of classified material maintained or criticality of area. List persons conducting evaluation.)
4. RESULTS: (Details on security measures in effect and any security weaknesses.)
5. RECOMMENDATIONS: (List recommendations to correct security weaknesses as they appear in paragraph 4. Reference paragraph for clarity.)

End of Report

CLASSIFICATION

REPORTED BY (Signature) Typed name of the senior person conducting the investigation and signature	APPROVED BY (Signature) Typed name and title of approving authority and signature

8. SAMPLE FORMAT FOR COUNTERINTELLIGENCE INSPECTION REPORT

COUNTERINTELLIGENCE REPORT (3850)
NAVMC 10481 (REV. 6-68)
Previous editions will not be used.

FILE NO. Control number
DATE Date report signed

CLASSIFICATION

SUBJECT Counterintelligence Inspection (Penetration, Vacated Command Post, Announced/Unannounced) Unit Parent Organization Location	REPORTING ORGANIZATION Complete organization identification and address
REFERENCES List pertinent references	DISTRIBUTION OF REPORT List organizations/agencies receiving copies of the report
	_____ ORIGIN OF REPORT Unit requesting/authority
ENCLOSURES List in order of report appearance	CASE CHARACTER/CATEGORY Counterintelligence Inspection
	PERIOD COVERED Inclusive dates of evaluation
	STATUS Closed/pending/referred/suspended

SYNOPSIS (Concise summary of the report.)

1. PREDICATION: (How the inspection was initiated.)

2. PURPOSE: (What the inspection was to determine and any limitations placed on the evaluation.)

3. BACKGROUND: (Information on previous inspections, criticality of the area, and/or coordination conducted. List persons conducting inspection.)

4. RESULTS: (Details of inspection and any security violations and/or hazards.)

5. RECOMMENDATIONS: (List recommendations to correct security violations and/or hazards.)

End of Report

CLASSIFICATION

REPORTED BY (Signature) Typed name of the senior person conducting the investigation and signature	APPROVED BY (Signature) Typed name and title of approving authority and signature

9. SAMPLE FORMAT FOR TECHNICAL SURVEILLANCE COUNTERMEASURES REPORT

COUNTERINTELLIGENCE REPORT (3850)
NAVMC 10481 (REV. 6-68)
Previous editions will not be used.

FILE NO. Control number
DATE Date report signed

CLASSIFICATION

SUBJECT Technical Surveillance Countermeasures Inspection/Survey Unit Parent Organization Location	REPORTING ORGANIZATION Complete organization identification and address
REFERENCES List pertinent references	DISTRIBUTION OF REPORT List organizations/agencies receiving copies of the report
	_____ ORIGIN OF REPORT Unit requesting/authority
ENCLOSURES List in order of report appearance	CASE CHARACTER/CATEGORY Technical Inspection/Survey
	PERIOD COVERED Inclusive dates of inspection/survey
	STATUS Closed/pending/referred/suspended

SYNOPSIS (Concise summary of the report.)

1. PREDICATION: (How the inspection/survey was initiated.)

2. PURPOSE: (What the inspection/survey was to determine and any limitations placed on the inspection/survey.)

3. BACKGROUND: (Information on previous inspections/surveys, the criticality of area, and the scope of the inspection/survey. List persons conducting inspection/survey.)

4. RESULTS:

   a. (Results of the inspection/survey and security measures required for the inspection/survey to remain valid.)
   b. (Security hazards noted.)

5. RECOMMENDATIONS: (List recommendations to correct security hazards as they appear in paragraph 4. Reference paragraph if required for clarity.)

End of Report

CLASSIFICATION

REPORTED BY (Signature) Typed name of the senior person conducting the investigation and signature	APPROVED BY (Signature) Typed name and title of approving authority and signature

Preparation of the Counterintelligence Report Form

1. To standardize and aid in report writing, the counterintelligence report normally contains five major sections: the predication, purpose, background, results, and comments or recommendations as appropriate.

2. The first page synopsizes when the report is longer than two pages. The synopsis is a concise summary of the pertinent information reported.

3. When the report is longer than one page, plain bond paper is used for additional pages. Additional pages are identified with the subject of the report, date, and file number located at the top of the page.

4. Subject block, if for a person, contains the surname (typed in uppercase) followed by the first and any other given names, rank, social security number, and complete military address. If the subject is a civilian, list occupation and civilian address. Date and place of birth are included for all persons. When the subject is an organization, the complete title is typed in uppercase followed by an abbreviated or short title that is used throughout the report. The address, if known, is also included in the subject block. When the report concerns an incident, the subject block answers, in order, three questions: what, where, and when (normal capitalization is used).

5. Enclosures to the counterintelligence report amplify or confirm information in the report. Items such as records, identification documents, statements, photographs, sketches, documents, and pamphlets may be used as enclosures when appropriate. Enclosures are identified in numerical order. In the body of the report, the enclosure designation follows immediately after referring to the item attached. The enclosure designation is typed in uppercase and placed in parentheses; e.g., (ENCLOSURE (2)).

6. Enclosures, references, and distribution are listed in the space provided. When space provided is insufficient, a separate page for each item is prepared and placed in numerical sequence following the last page of the basic report.

7. Reports normally are written in narrative style, third person, simple past tense, and active voice, except when quoting a source or when describing a state of mind or condition. Simple, direct, standard English is used for ease of comprehension and to reduce misinterpretation. Expressions reflecting approval or disapproval of occurrences, persons, or objects being described by the person writing the report are prohibited. The report must contain the information that was obtained, not how it was obtained. Means techniques to develop information are not incorporated into the report, except as prescribed in the case of counterintelligence surveys, evaluations, and inspections.

8. Comments by counterintelligence personnel are used to aid in the study and evaluation of the information reported. Comments are placed at the end of the report/interview/interrogation or separate phase of the report in the case of surveys, evaluation, or inspections. Comments are identified clearly and contain only the views of the person preparing the report. All pertinent information obtained must be stated in the body of the report.

9. Once military personnel have been identified fully in the report, they are referred to then by their rank (abbreviated) and surname. Civilian personnel, after full identification, are referred to by surname only. This procedure is followed unless more than one person with the same surname is referred to in the report.

Appendix C

Sample Format for Counterintelligence Estimate

CLASSIFICATION

Copy no. ___ of ___ copies
Issuing headquarters
PLACE OF ISSUE
Date/time of issue

COUNTERINTELLIGENCE ESTIMATE (Number)

Ref: Maps, charts, and/or other relevant documents

1. ( ) MISSION

State the assigned or assumed mission.

2. ( ) AREA OF OPERATIONS

This paragraph discusses characteristics of the area and their effect on enemy intelligence, sabotage, subversive, and terrorist operations and on our counterintelligence operations and measures.

a. ( ) Weather

(1) ( ) Existing situation.

(2) ( ) Effect on enemy intelligence, sabotage, subversive, and terrorist operations.

(3) ( ) Effect on our counterintelligence operations and measures.

b. ( ) Terrain. Analyze under the same headings as weather.

c. ( ) Other Characteristics. Additional pertinent characteristics are considered in separate subparagraphs: sociological, political, economic, psychological, and other factors. Other factors may include, but are not limited to: telecommunication material, transportation, manpower, hydrography, science, and technology. These are analyzed under the same headings as weather.

Page number

CLASSIFICATION

CLASSIFICATION

3. ( ) INTELLIGENCE, SABOTAGE, SUBVERSIVE, AND TERRORIST SITUATION

Discusses enemy intelligence, sabotage, subversive, and terrorist activities as to the current situation and recent/significant activities. Included are known factors on enemy intelligence, sabotage, subversive, and terrorist organizations. Fact sheets containing pertinent information on each organization may be attached to the estimate as annexes.

a. ( ) Location and disposition.

b. ( ) Composition.

c. ( ) Strength, including local available strength, availability of replacements, efficiency of enemy intelligence, sabotage, subversive, and terrorist organizations.

d. ( ) Recent and present significant intelligence, sabotage, and subversive activities/movement (including enemy knowledge of our intelligence and counterintelligence efforts).

e. ( ) Technical capabilities and equipment.

f. ( ) Peculiarities and weaknesses.

g. ( ) Other factors.

4. ( ) INTELLIGENCE, SABOTAGE, SUBVERSIVE, AND TERRORIST CAPABILITIES

a. ( ) List all capabilities as follows:

(1) ( ) Intelligence. (Include all known/estimated enemy methods.)

(2) ( ) Sabotage. (Include all possible agent/guerrilla capabilities for military, political, and economic sabotage.)

(3) ( ) Subversion. (Include all types, such as propaganda, sedition, treason, disaffection, and threatened terrorists activities affecting our troops, allies, and local civilians, and assistance in the escape and evasion of hostile civilians.)

(4) ( ) Terrorist. (Include capabilities of terrorist personalities and organizations in area of operation.)

b. ( ) Analysis and discussion of enemy capabilities for intelligence, sabotage, subversive, and terrorism, as a basis to judge the probability of their adoption.

5. ( ) CONCLUSIONS

a. ( ) Probability of enemy adoption of intelligence, sabotage, subversive, and terrorist programs or procedures based on capabilities.

Page number

CLASSIFICATION

CLASSIFICATION

b. ( ) Effects of enemy capabilities on our course of action.

c. ( ) Effectiveness of our own counterintelligence measures and additional requirements or emphasis needed.

Signature
Name
Rank and Service

ANNEXES:

DISTRIBUTION:

Page number

CLASSIFICATION

Appendix D

Partially Completed Counterintelligence Measures Worksheet

UNITS: I MAF

Period Covered: From 161800D Aug to Seizure of Force Beachhead

(1) Phases or Periods of the Operation	(2) Categories of Counterintelligence Activities Involved	(3) Counterintelligence Measures to be Adopted	Agencies Responsible for Execution of Counterintelligence Measures												(5) Instructions Regarding Entries in Columns (3) and (4), Notes for Future Action, and Staff Coordination Measures
			Civil Affairs	CEO	Public Info/Off	Provost Marshal	Comm/Intel Unit	All Units	CI Team						
Assault Phase	1. MILITARY SECURITY a. Security discipline.	(1) Cover or paint all vehicle and aircraft markings.						X							Coordinate with G-4. Provost Marshal report violations.
		(2) Remove identification from uniform.						X							Coordinate with G-1. Provost Marshal report violations.
		(3) Restrict personnel to area except when on official business.						X							
		(4) Emphasize security discipline in command posts, and elsewhere, with particular reference to handling of documents and maps, phone conversations, loose talk, and speculation which might convey information to the enemy. All personnel will be instructed regarding same.						X							Coordinate with G-3. CI team assist with instruction and check.
		(5) Report all breaches and suspected compromise of security at once to G-2.				X	X	X	X						SOP
	b. Security of nuclear weapons and delivery systems.	(6) Disseminate location of nuclear weapons on need-to-know basis.		X											Coordinate with G-1, G-3, and G-4.
		(7) Nuclear weapons units draw all supplies from division distribution points by use of own vehicles.													Coordinate with G-4.
		(8) Collect and place under guard or evacuate as determined appropriate by unit commander, civilians in position to observe nuclear weapons storage and delivery sites.	X			X			X						Coordinate with G-1
	c. Safeguarding of classified defense information and equipment.	(9) Check SOP plans for security of cryptographic devices, for destruction, and for report of loss or compromise.		X			X	X	X						SOP. CI team check.
		(10) Check plans and equipment for destruction of documents in event of imminent capture.		X				X	X						SOP. CI team check.
	d. Communications security.	(11) Use authorized call signs, authenticators, and shackle codes.		X			X	X							SOP. Comm/Intel unit check.
		(12) Check that unauthorized personnel are prohibited from entering message centers.		X				X	X						SOP
		(13) Patrol all wire lines used by units of division		X				X							SOP. Check with CEO for compliance.
		(14) Cut all wire lines leading into enemy-occupied territory		X				X							Coordinate with CATF.
	e. Security of troop movements	(15) Control the movement of all vehicles and aircraft to the extent that a change in normal operations is not indicated.						X							Coordinate with G-3 and G-4 Provost Marshal report violations.

Appendix E

JOPS Format for a Counterintelligence Appendix

CLASSIFICATION

Command
Address
Date

APPENDIX 3 TO ANNEX B TO ANY COMMAND OPLAN NUMBER (U)
COUNTERINTELLIGENCE (U)

(U) REFERENCES: List pertinent command or Service directives and counterintelligence products.

1. ( ) GENERAL

a. ( ) General objectives and guidance necessary to accomplish the mission.

b. ( ) General statement of command responsibilities and reporting procedures to ensure the flow of pertinent counterintelligence information to higher, adjacent, or subordinate commands.

c. ( ) General statement of responsibility for coordination and liaison between counterintelligence elements of the United States and those of its allies, or between other commands and agencies.

d. ( ) General statement of the effect of U.S. Statutes, Executive Orders, DOD Directives, and Status- of-Forces Agreements on counterintelligence activities.

2. ( ) HOSTILE THREAT. Summarize the enemy situation regarding their intelligence collection, sabotage, terrorism, and subversion efforts and discuss it in light of the current enemy activities and capabilities which stem from known enemy training and doctrine.

3. ( ) COUNTERINTELLIGENCE ORGANIZATIONS AND UNITS

a. ( ) Identify the required counterintelligence organizations or units of the U.S. Army, U.S. Navy, or U.S. Air Force, and their approximate strengths.

CLASSIFIED BY:
DATE FOR ( ) DECLASSIFICATION
OR ( ) REVIEW
IS:
EXTENDED BY:

Page number

CLASSIFICATION

CLASSIFICATION

b. ( ) Identify specific requirements for language and technical skills; e.g., polygraph operators, DAME and DASE technicians, etc.

4. ( ) SECURITY. Provide planning guidance concerning procedures and responsibilities for the following security activities:

a. ( ) Force or Unit Headquarters

b. ( ) Military Security

c. ( ) Civil Security

d. ( ) Port, Frontier, and Travel Security

e. ( ) Safeguarding Classified Information and Codes

f. ( ) Security Discipline and Security Education

g. ( ) Protection of Critical Installations

h. ( ) Special Weapons Security

i. ( ) Counterterrorist Measures

5. ( ) WARTIME INFORMATION SECURITY PROGRAM

a. ( ) Categories. Identify type of WISP to be implemented; e.g., Armed Forces WISP, Field Press WISP, etc.

b. ( ) Implementation. Identify conditions for implementation for each category of WISP.

c. ( ) Responsibilities. Identify the staff or other element that will initiate the implementation.

6. ( ) COUNTERINTELLIGENCE PLANS, ACTIVITIES, AND FUNCTIONS

a. ( ) Defensive. Identify the staff or the commands that have supporting counterintelligence assets and provide planning guidance concerning procedures, priorities, and channels for handling:

(1) ( ) Interrogation of enemy prisoners of war and defectors.

(2) ( ) Screening of indigenous refugees, displaced persons, and detained suspects.

(3) ( ) Debriefing of U.S. or other friendly personnel who evade, escape, or are released from enemy control.

(4) ( ) Exploitation of captured documents and material.

Page number

CLASSIFICATION

CLASSIFICATION

b. ( ) Offensive. Establish guidance, to include control and coordination, for approval of counterespionage, countersabotage, countersubversion, double agent, counterterrorist, deception, or other special operations.

7. ( ) COUNTERINTELLIGENCE TARGETS AND REQUIREMENTS

a. ( ) Targets. Provide guidance to subordinate commands for developing counterintelligence targets based on an assessment of the overall counterintelligence threat. Designate priorities that emphasize the relative importance of the following counterintelligence target categories:

(1) ( ) Personalities; include responsibilities for developing "black," "gray," and "white" lists.

(2) ( ) Installations.

(3) ( ) Organizations and groups.

(4) ( ) Documents and material.

b. ( ) Identify special counterintelligence collection requirements and priorities to be fulfilled by counterintelligence operations.

c. ( ) Identify any other command information required.

8. ( ) COUNTERINTELLIGENCE PRODUCTION AND DISSEMINATION. Provide guidance for the analysis, production, and dissemination of counterintelligence from all sources.

9. ( ) COORDINATION

a. ( ) Identify coordination requirements peculiar to the counterintelligence activities listed in paragraphs 6 through 8, above.

b. ( ) Identify coordination requirements for counterintelligence support from other U.S. units or agencies.

10. ( ) MISCELLANEOUS. Include any necessary guidance not provided above; e.g., intelligence contingency fund accounting, reporting, and restrictions.

JOPS Format for a Human Intelligence (HUMINT) Resources Appendix

CLASSIFICATION

Command
Address
Date

APPENDIX 5 TO ANNEX B TO (COMMAND) OPLAN XXXX (U)
HUMAN INTELLIGENCE RESOURCES (U)

(U) REFERENCES: List applicable DIA, Service, and command regulations, directives, collateral, or supporting plans, studies, manuals, and estimates.

1. ( ) GENERAL

a. ( ) Provide the general objectives and guidance necessary for accomplishment of the mission.

b. ( ) Provide a statement of command responsibilities and the chain of command for reporting channels.

2. ( ) HUMINT ORGANIZATION. Identify the HUMINT organizations and approximate strengths of units required.

3. ( ) COLLECTION ACTIVITIES, FUNCTIONS, AND PLANS. For each activity or separate HUMINT function applicable to the operation, identify the staff, element, or unit responsible and the type of collection plans and approving authority required.

4. ( ) COLLECTION REQUIREMENTS

a. ( ) Refer to Appendix 1 (Essential Elements of Information) to Annex B (Intelligence), if applicable.

b. ( ) Identify targets and other collection requirements to be fulfilled by HUMINT operations.

5. ( ) COORDINATION

a. ( ) Identify coordination requirements peculiar to HUMINT operations. Refer to activities listed in paragraph 3 above, if applicable.

b. ( ) Identify coordination requirements for support from other units or agencies.

(1) ( ) Support requirements from other U.S. Government Agencies.

(2) ( ) Counterintelligence coordination:

CLASSIFICATION

(a) ( ) To obtain technical and security support.

(b) ( ) To provide mutual support to satisfy collection requirements. (See par. 3 above.)

(3) ( ) Communication support required for conduct of HUMINT operations.

c. ( ) Coordinate HUMINT operations with UW, PSYOP, E&E, and deception.

6. ( ) MISCELLANEOUS. Include other items not mentioned above, such as intelligence contingency funds accounting, reporting, and restrictions. Identify any special reports required and the channels for submitting them.

Page number

CLASSIFICATION

Appendix F

Format for a Counterintelligence Plan

CLASSIFICATION

Copy no. ___ of ___ copies
Issuing Headquarters
PLACE OF ISSUE
Date/time of issue

APPENDIX 3 TO ANNEX B TO OPLAN XXXX (U)
COUNTERINTELLIGENCE PLAN (U)

Ref: (a) Maps, charts, and related documents

1. ( ) PURPOSE

To provide planning guidance concerning procedures and the responsibilities of commanders for counterintelligence activities within their area of responsibility.

2. ( ) MISSION

State the counterintelligence mission.

3. ( ) EXECUTION

Assign tasks to counterintelligence units and/or staff officers under the command of the headquarters. In assigning tasks, the following factors are considered:

a. ( ) Provision for the flow of pertinent counterintelligence information to higher, adjacent, and subordinate commands.

b. ( ) Effects of status of forces agreements on counterintelligence operations and collection.

c. ( ) Liaison and coordination with counterintelligence and security elements of other commands and organizations.

d. ( ) Security considerations for personnel, information, and installations.

Page number

CLASSIFICATION

CLASSIFICATION

4. ( ) MILITARY SECURITY

a. ( ) Reference to current standing operating procedure.

b. ( ) Special safeguarding of classified military information and equipment at headquarters and in the field.

c. ( ) Security of troop movements and concentrations.

d. ( ) Countersigns.

e. ( ) Communications security.

f. ( ) Security discipline and training.

g. ( ) Censorship (refer to paragraph 7 as necessary).

h. ( ) Counterespionage.

i. ( ) Countersabotage.

j. ( ) Countersubversion.

k. ( ) Counterterrorism.

l. ( ) Tactical measures as required, including concealment and counterreconnaissance.

m. ( ) Special handling of prisoners-of-war of counterintelligence interest.

n. ( ) Special handling of enemy agents and security risks not normally classified as prisoners of war.

o. ( ) Special handling of military evaders and escapees.

p. ( ) Security control of friendly secret agents and relations with resistance groups operating in enemy controlled territory.

q. ( ) Security control of visitors, including press representatives and photographers.

r. ( ) Security control of prohibited, regulated, and restricted areas.

s. ( ) Protection of commanders and other personnel performing critical duties or possessing sensitive information.

Page number

CLASSIFICATION

CLASSIFICATION

t. ( ) Reports of security violations.

u. ( ) Counterintelligence targets (enemy military).

5. ( ) CIVIL SECURITY

a. ( ) Registration of civilians in objective area.

b. ( ) Control of circulation.

c. ( ) Passes and permits.

d. ( ) Curfew (hours, enforcement responsibility, and procedures).

e. ( ) Labor (registration, screening, and security control).

f. ( ) WISP (civilian) (refer to paragraph 7 as necessary).

g. ( ) Surveillance of suspect political groups.

h. ( ) Communication monitoring.

i. ( ) Diplomatic personnel control (neutral, friendly, and hostile).

j. ( ) Security control of refugees and displaced persons.

k. ( ) Interrogation and detention centers.

l. ( ) Control and utilization of civilian police agencies.

m. ( ) Security control of prohibited, regulated, and restricted areas.

n. ( ) Protection of friendly civil leaders.

o. ( ) Counterespionage.

p. ( ) Countersabotage.

q. ( ) Countersubversion.

r. ( ) Counterterrorism.

s. ( ) Counterintelligence target lists.

(1) ( ) Installations and facilities.

(2) ( ) Black, gray, and white lists (civilian personnel known to be hostile or dangerous, possibly hostile or where sentiments are not known, and personnel openly friendly to us).

CLASSIFICATION

6. ( ) EMBARKATION SECURITY

a. ( ) Jurisdictional responsibilities of Marine, Navy, Army, Air Force, allied, and civil authorities.

b. ( ) Security control of embarkation areas including:

(1) ( ) Control of harbor traffic.

(2) ( ) Merchant seaman control.

(3) ( ) Stevedores, pilots, and dockhands (screening and control).

(4) ( ) Counterespionage, countersabotage, and countersubversion.

(5) ( ) Action taken against suspects.

7. ( ) WARTIME INFORMATION SECURITY PROGRAM (WISP)

a. ( ) Area and unit policy.

b. ( ) WISP objectives.

c. ( ) Press briefings prior to embarkation and movement to the objective.

d. ( ) Types of releasable and nonreleasable information.

e. ( ) Special surveillance.

f. ( ) Prisoner-of-war and internee censorship.

g. ( ) Control of civilian communications, press, and radio in objective area.

h. ( ) Responsibilities for civil censorship.

i. ( ) Evaluation and dissemination of information derived from censorship.

j. ( ) Reports of violations.

8. ( ) SPECIAL OPERATIONS

a. ( ) Types of operations to be initiated and unit assignments.

b. ( ) Coordination and approval required for subsequent operations.

Page number

CLASSIFICATION

CLASSIFICATION

9. ( ) ADMINISTRATION AND LOGISTICS

a. ( ) Counterintelligence teams/personnel; availability, and allocation.

b. ( ) Counterintelligence credentials; issue, control, and applicability.

c. ( ) Counterintelligence funds; availability, use, and accounting for.

d. ( ) Counterintelligence reports and reporting channels.

e. ( ) Special counterintelligence training which may be required.

f. ( ) Other instructions.

Signature
Name
Rank and Service
Commanding

(or) BY COMMAND OF . . . Rank and Name

Signature
Name
Rank and Service
Chief of Staff

TABS:

DISTRIBUTION:

Page number

CLASSIFICATION

Appendix G

Sample Format for Counterintelligence Reduction Plan

PERSONALITY/INSTALLATION: Operation Bold Lighting MAP REF: Name, Series, Sheet(s)

TARGET NO.	TARGET	LOCATION / DESCRIPTION	PRIORITY	SUBTEAM ASSIGNMENT	SPECIAL INSTRUCTIONS	INTERESTED AGENCIES
1	Broadcasting Station	Grid Coordinates/3 km NW of city on Victory Road	1	1	Locate/take into custody Station State Security Officer and all propaganda file material	G-5/PAO
2	Government Control Center	Grid Coordinates/Largest building in city center, gable roof	3	1	Ensure file information protected for further analysis	G-5
3	Military Intelligence Headquarters	Grid Coordinates/Located on Liberation Military Compound E of city	1	2	Locate/search CI and Agent Operations Section	Task Force N2
4	Smith, John Q Intelligence Cadre	Grid Coordinates/Military Intelligence Headquarters (above). Home address: 134 6th St, Apt 3B	2	2	Potential Defector; Handle accordingly	10th Army MI
5	Infiltration Training Facility	Grid Coordinates/Located W of city on Seaward Peninsula	3	2	Secure. Search for file information on personalities and operations. Coordinate with Task Force N-2	Task Force N2
6	Political Prison	Grid Coordinates/Triangular-shaped compound enclosed by 20-foot block wall bordered by Liberation Ave, 9th St, and Bay	2	1	Personalities of CI interest on separate listing. Provide list of recovered personalities to HQ via most expedient means	G-5
7	National Intelligence Field Office	Grid Coordinates/Located in concrete block building on corner of 5th St and Liberation Ave	1	2	Immediately evaluate all documents/equipment	G-2

Instructions for Completing Counterintelligence Reduction Plan

TARGET NO: Consecutively marked by logical sequence.

TARGET: Personality or installation such as John Smith, Intelligence Officer; Intelligence Training Facility; National Intelligence Field Office; Government Control Center; Broadcasting Station.

LOCATION: Grid coordinates. If urban environment, also use street address if available. Example: 134 Eighth Street, Apartment 3B; located on Liberation Military Compound east of city; 3 kilometers west of city on Victory Road; located corner of Fifth Street and Revolution Avenue.

DESCRIPTION: Physical characteristics of personality such as height, weight, distinguishing characteristics, or description of installation such as largest building in city center, triangular-shaped compound, concrete block building.

PRIORITY: Priority One. Those targets which represent the greatest security threat or which possesses the largest potential source of intelligence or counterintelligence information or material, and are to be exploited or neutralized as soon as possible.

Priority Two. Those targets which are of a lesser significance than priority one and are to be taken under control after priority one targets have been neutralized or exploited.

Priority Three. Those targets which are of a lesser significance than priority one or two and are neutralized or exploited as time and personnel permit.

SUBTEAM ASSIGNMENT: Subteam to which target is assigned for neutralization or exploitation.

SPECIAL INSTRUCTIONS: Pertinent action which should be taken in neutralization/exploitation of target (e.g., locate and search counterespionage and agent operations section; potential defector, handle accordingly; immediately evacuate all documents and equipment).

INTERESTED AGENCIES: List internal and external agencies which have primary interest (e.g., PAO, G-5, task force N2, Army MI, CIA, etc.).

Index